# bitdefender
# ANTIVIRUS PRO 2011

## Manual do Utilizador

Copyright© 2010 BitDefender

# BitDefender Antivirus Pro 2011
*Manual do Utilizador*

Publicado 2010.08.09

Copyright© 2010 BitDefender

## Aviso Legal

Todos os direitos reservados. Nenhuma parte deste livro pode ser reproduzida ou transmitida de qualquer forma ou por quaisquer meios, electrónicos ou mecânicos, incluindo fotocópias, gravação, ou qualquer sistema de arquivo de informação, sem a permissão por escrito de um representante autorizado de BitDefender. A inclusão de pequenas frases do texto em comparativas poderão ser feitas desde que seja feita a menção da fonte da frase em questão. O conteúdo não pode ser de forma alguma modificado.

**Aviso e Renúncia.** Este produto e a sua documentação estão protegidas por direitos de autor. A informação neste documento é apresentada numa base de "tal como é", sem qualquer garantia. Apesar de todas as precauções terem sido tomadas na preparação deste documento, os autores não serão responsabilizados por qualquer pessoa ou entidade com respeito a qualquer perda ou dano causado ou alegadamente causado directa ou indirectamente pela informação contida neste livro.

Este livro contém links para Websites de terceiras partes que não estão baixo controlo da BitDefender, e a BitDefender não é responsável pelo conteúdo de qualquer site acedido por link. Se aceder a um site de terceiras partes mencionado neste manual, faz isso à sua própria conta e risco. A BitDefender fornece esses links apenas para facilitar, e a inclusão do link não implica que a BitDefender endosse ou aceite qualquer responsabilidade pelo conteúdo deste sites de terceiras partes.

**Marcas Registadas.** Nomes de Marcas Registadas poderão aparecer neste livro. Todas as marcas registadas ou não registadas neste documento são da exclusiva propriedade dos seus respectivos proprietários.

bitdefender

# Índice

Instalação e Remoção ..... 1

1. Requisitos de Sistema ..... 2
1.1. Requisitos Minímos do Sistema ..... 2
1.2. Requisitos de sistema recomendados ..... 2
1.3. Requisitos de Software ..... 2

2. A preparar a Instalação ..... 4

3. Instalar BitDefender ..... 5
3.1. Passo 1 - Introdução ..... 5
3.2. Passo 2 - Preparar a Instalação ..... 5
3.3. Passo 3 - Registo ..... 6
3.4. Passo 4 - Escolher o Modo ..... 9
3.5. Passo 5 - Configurar ..... 10
3.6. Passo 6 - Opções de Suporte ..... 13
3.7. Passo 7 - Confirmar ..... 14
3.8. Passo 8 - Terminar ..... 14

4. Fazer o Upgrade de Versões Anteriores do BitDefender ..... 15

5. Remover ou Reparar o BitDefender ..... 16

Introdução ..... 17

6. Apresentação ..... 18
6.1. A abrir o BitDefender ..... 18
6.2. Icon da Barra de Tarefas ..... 18
6.3. Barra de Actividade da Análise ..... 19
6.3.1. Analisar Ficheiros e Pastas ..... 20
6.3.2. Desactivar/Restaurar Barra de Actividade da Análise ..... 20
6.4. Detecção Automática de Dispositivos ..... 21

7. Janela Principal da Aplicação ..... 23
7.1. Modo Básico ..... 23
7.1.1. Estado da Área ..... 24
7.1.2. Área Proteja o seu PC ..... 24
7.1.3. Área de Ajuda ..... 25
7.2. Modo Intermédio ..... 25
7.2.1. Painel ..... 26
7.2.2. Segurança ..... 27
7.2.3. REDE ..... 28
7.3. Modo Avançado ..... 28

8. Ferramentas ..... 30

9. Alertas e Pop-ups ..... 33
9.1. Alertas Antivírus ..... 33
9.2. Alertas do Controlo Activo de Vírus ..... 34

9.3. Alertas de Detecção de Dispositivo ... 34
9.4. Alertas Antiphishing ... 35
9.5. Alertas do Controlo de Privacidade ... 36
9.5.1. Alertas de Registo ... 36
9.5.2. Alertas de Script ... 37
9.5.3. Alertas de Cookie ... 37
10. Reparar Incidência ... 38
10.1. Assistente Reparar Incidências ... 38
10.2. Configurar os Alertas de Estado ... 39
11. Configurar Definições Principais ... 41
11.1. Opções de Segurança ... 41
11.2. Definições de Alertas ... 42
11.3. Configuração Geral ... 43
11.4. Reconfigurar o Perfil de Utilização ... 44
12. Histórico e Eventos ... 46
13. Registo e a Minha Conta ... 47
13.1. Registar BitDefender Antivirus Pro 2011 ... 47
13.2. A activar o BitDefender ... 48
13.3. Adquirir ou Renovar Chaves de Licença ... 50
Configuração e Gestão ... 51
14. Configuração Geral ... 52
15. Protecção Antivírus ... 56
15.1. Protecção em Tempo-real ... 56
15.1.1. Ajustar o Nível de Protecção em Tempo Real ... 57
15.1.2. Criar um Nível de Protecção Personalizado ... 58
15.1.3. Alterar as Acções Aplicadas aos Ficheiros Detectados ... 59
15.1.4. Restaurar as Predefinições ... 60
15.1.5. Configurar o Controlo Activo de Vírus ... 61
15.1.6. Configurar o Sistema de Detecção de Intrusão: ... 63
15.2. Análise a-pedido ... 63
15.2.1. Analisar Ficheiros e Pastas ... 64
15.2.2. Assistente de Análise Antivírus ... 65
15.2.3. Ver os Relatórios da Análise ... 68
15.2.4. Gerir Tarefas de Análise Existentes ... 68
15.3. Configurar Exclusões da Análise ... 75
15.3.1. Excluir Ficheiros ou Pastas da Análise ... 76
15.3.2. Excluir Extensões de Ficheiros da Análise ... 77
15.3.3. Gerir Exclusões da Análise ... 78
15.4. Àrea de Quarentena ... 78
16. Protecção Antiphishing ... 81
16.1. Configurar a Lista Branca de Antiphishing ... 81
16.2. Gerir a Protecção Antiphishing do BitDefender no Internet Explorer e Firefox ... 81

17. Consultor de Procura ..... 83
17.1. Desactivar o Consultor de Procura: ..... 83
18. Controlo de Privacidade ..... 84
18.1. Configurar Nível de Protecção ..... 84
18.2. Controlo de identidade ..... 85
18.2.1. Sobre o Controlo de Identidade ..... 85
18.2.2. Configurar o Controlo de Identidade ..... 86
18.2.3. Gerir Regras ..... 89
18.3. Controlo de registo ..... 89
18.4. Controlo de cookies ..... 90
18.5. Controlo de script ..... 91
19. Vulnerabilidade ..... 93
19.1. A analisar em busca de Vulnerabilidades ..... 93
19.2. Estado ..... 94
19.3. Definições ..... 94
20. Encriptação de Chat ..... 96
20.1. Desactivar a Encriptação para Utilizadores Específicos ..... 97
20.2. Barra de Ferramentas do BitDefender na Janela de Conversação ..... 97
21. Modo de Jogo / Portátil ..... 98
21.1. Modo de Jogo ..... 98
21.1.1. Configurar Modo de Jogo Automático ..... 99
21.1.2. Gerir a Lista de Jogos ..... 99
21.1.3. Adicionar ou Editar Jogos ..... 100
21.1.4. Configurar as Definições do Modo de Jogo ..... 100
21.1.5. Mudar a Tecla de Atalho do Modo de Jogo ..... 100
21.2. Modo Portátil ..... 101
21.2.1. Configurar Definições do Modo de Portátil ..... 101
21.3. Modo Silêncio ..... 101
21.3.1. Configurar a Acção em Ecrã Completo ..... 102
21.3.2. Configurar as Definições do Modo Silêncio ..... 102
22. A Sua Rede ..... 103
22.1. Activar a Rede BitDefender ..... 103
22.2. Adicionar Computadores à Rede BitDefender ..... 104
22.3. Gerir a Rede BitDefender ..... 104
23. Actualização ..... 107
23.1. Efectuar uma Actualização ..... 107
23.2. Configurar Definições de Actualização ..... 108
23.2.1. Configuração da Localização da Actualização ..... 109
23.2.2. Configurar Actualização Automática ..... 109
23.2.3. Configurar Actualização Manual ..... 110
23.2.4. Configuração Avançada ..... 110
Como ..... 111
24. Como Posso Analisar Ficheiros e Pastas? ..... 112

24.1. Usar o Menu Contextual do Windows ..... 112
24.2. Usar Tarefas de Análise ..... 112
24.3. Usando a Barra de Actividade da Análise ..... 113
25. Como Posso Criar Uma Tarefa de Análise Personalizada? ..... 115
26. Como Posso Agendar uma Análise ao Computador? ..... 117
27. Como Posso Actualizar o BitDefender Através de um Proxy? ... 119
28. Como Posso Fazer o Upgrade para Outro Produto do BitDefender 2011? ..... 120
Troubleshooting e Obter Ajuda ..... 121
29. Solução de problemas ..... 122
29.1. Problemas de Instalação ..... 122
29.1.1. Erros de Validação da Instalação ..... 122
29.1.2. Falha na Instalação ..... 123
29.2. O meu sistema parece estar lento ..... 124
29.3. A Análise Não Inicia ..... 125
29.4. Já Não Consigo Utilizar uma Aplicação ..... 125
29.5. Como Actualizar o BitDefender numa Ligação à Internet Lenta ..... 126
29.6. O Meu Computador Não Está Ligado à Internet. Como Posso Actualizar o BitDefender? ..... 127
29.7. Os serviços BitDefender não estão a responder ..... 127
29.8. A Desinstalação do BitDefender Falhou ..... 128
30. Remover Malware do Sistema ..... 129
30.1. CD de Emergência BitDefender ..... 129
30.2. O Que Fazer Se o BitDefender Encontrar Vírus No Seu Computador? ..... 130
30.3. Como Posso Limpar o Vírus de um Arquivo? ..... 131
30.4. Como Posso Limpar o Vírus de um Arquivo de Correio Electrónico? ..... 132
30.5. Como Posso Analisar o Computador no Modo de Segurança? ..... 133
30.6. O Que Fazer Se o BitDefender Identificou um Ficheiro Limpo como Infectado? ..... 134
30.7. Como Limpar os Ficheiros Infectados da Informação de Volume de Sistema ..... 134
30.8. O que são Ficheiros Protegidos por Palavra-Passe no Relatório de Análise? ..... 136
30.9. O Que São os Itens Ignorados no Relatório de Análise? ..... 136
30.10. O que são os Ficheiros Sobre-Comprimidos no Relatório de Análise? ..... 136
30.11. Porque é que o BitDefender eliminou automaticamente um ficheiro infectado? ..... 136
31. Apoio ..... 138
31.1. Recursos Em Linha ..... 138
31.1.1. Base de Conhecimento do BitDefender ..... 138
31.1.2. Fórum de Suporte BitDefender ..... 138
31.1.3. Portal Malware City ..... 139
31.1.4. Tutoriais ..... 139

31.2. Pedir Ajuda ..... 140
32. Contactos ..... 142
32.1. Endereços Web ..... 142
32.2. Distribuidores Locais ..... 142
32.3. Escritórios BitDefender ..... 143
33. Informações Úteis ..... 145
33.1. Como Posso Remover Outras Soluções de Segurança? ..... 145
33.2. Como Posso Reiniciar no Modo de Segurança? ..... 146
33.3. Estou a Utilizar uma Versão de 32 ou 64 Bit do Windows? ..... 146
33.4. Como Posso Encontrar as Minhas Definições de Proxy? ..... 147
33.5. Como Posso Remover Totalmente o BitDefender? ..... 147
33.6. Como Posso Activar/Desactivar a Protecção Em Tempo Real ..... 147
33.7. Como Posso Mostrar Objectos Ocultos no Windows? ..... 148
Glossário ..... 149

# Instalação e Remoção

# 1. Requisitos de Sistema

Só pode instalar o BitDefender Antivirus Pro 2011 nos computadores que tenham os seguintes sistemas operativos:

- Windows XP com Service Pack 3 (32 bit) / Windows XP com Service Pack 2 (64 bit)
- Windows Vista com Service Pack 1 ou superior (32/64 bit)
- Windows 7 (32/64 bit)

Antes da instalação, certifique-se que o seu computador cumpre com os requisitos mínimos de hardware e software.

Nota

Para ficar a saber que sistemo operativo o seu computador contém e a informação de hardware do mesmo, clique com o botão direito do rato no ícone **Meu Computador** no Ambiente de Trabalho e depois seleccione **Propriedades** do menu.

## 1.1. Requisitos Minímos do Sistema

- 1 GB de espaço disponível em disco
- Processador de 800 MHz
- Memória RAM:
  - 512 MB para o Windows XP
  - 1 GB para o Windows Vista e Windows 7
- Internet Explorer 6.0
- .NET Framework 2 (também disponível no kit de instalação)
- Adobe Flash Player 10.0.45.2

## 1.2. Requisitos de sistema recomendados

- 1 GB de espaço disponível em disco
- Processador Intel Core Duo (1,66 GHz) ou equivalente
- Memória RAM:
  - 1 GB para o Windows XP e Windows 7
  - 1.5 GB para Windows Vista
- Internet Explorer 7
- .NET Framework 2 (também disponível no kit de instalação)
- Adobe Flash Player 10.0.45.2

## 1.3. Requisitos de Software

A protecção antiphising está disponível apenas para:

- Internet Explorer 6.0 ou superior
- Mozilla Firefox 3.x
- Yahoo! Messenger 8.1

- Microsoft Windows Live Messenger 8

Encriptação para Instant Messaging (IM) está disponível para:

- Yahoo! Messenger 8.1
- Microsoft Windows Live Messenger 8

# 2. A preparar a Instalação

Antes de instalar o BitDefender Antivírus 2010, complete estes procedimentos para assegurar uma boa instalação:

- Assegure-se que o computador onde vai instalar o BitDefender contém os requisitos minimos do sistema.Se o seu computador não contém os requisitos mínimos do sistema, o BitDefender não será instalado ou, se instalado, não trabalhará correctamente e provocará lentidão e instabilidade no sistema.Para ver a lista completa dos requisitos mínimos do sistema, por favor consulte o "*Requisitos de Sistema*" (p. 2).
- Ligue-se ao computador utilizando uma conta de Administrador.
- Remova quaisquer outros softwares de segurança do seu computador.Executar dois programas de segurança simultaneamente poderá afectar o seu funcionamento e causar grandes problemas no sistema.Por defeito, o Windows Defender será desactivado antes da instalação começar.

# 3. Instalar BitDefender

Pode instalar o BitDefender a partir do CD de instalação do BitDefender ou utilizando o ficheiro de instalação descarregado do site da BitDefender ou de outros sites autorizados (por exemplo, de sites de parceiros da BitDefender ou de uma loja on-line).Pode descarregar o ficheiro de instalação do site da BitDefender seguindo este endereço: http://www.bitdefender.com/site/Downloads/.

- Para instalar o BitDefender a partir do CD, insira o CD na drive. Uma janela de boas-vindas aparecerá em alguns momentos. Siga as instrucções e começe a instalação.

  Nota

  O écran de boas-vindas dá-lhe a opção de copiar o pacote de instalação do CD para uma pen USB. Isto é útil se necessitar de instalar o BitDefender num computador que não tem uma drive de CD (por exemplo um netbook).Insira a pen USB na drive respectiva e depois clique em **Copiar para a USB**.Depois, vá até ao computador sem a drive de CD, insira a pen USB e faça duplo-clique no ficheiro `runsetup.exe` que se encontra na pasta onde guardou o pacote de instalação.

  Se o ecrã de boas-vindas não aparecer, vá ao directório-raiz do CD e faça duplo clique em `autorun.exe`.

- Para instalar o BitDefender utilizando um ficheiro de instalação descarregado, localize o ficheiro e faça duplo-clique sobre ele.

O instalador irá primeiro verificar o seu sistema para validar a instalação.Se a instalação for válida, ser-lhe-á pedido que seleccione o idioma antes de aparecer o assistente de configuração.

O assistente vai ajudar a instalar o BitDefender no seu computador e, ao mesmo tempo, vai permitir-lhe configurar as definições principais e o interface de utilizador.

## 3.1. Passo 1 - Introdução

Por favor, leia o Acordo de Licença e seleccione **Ao assinalar esta caixa, acito o cordo de licença do BitDefender**.Clique em **Seguinte** para continuar.

Se não concordar com estes termos clique em **Cancelar**. O processo de instalação será cancelado e terminará.

## 3.2. Passo 2 - Preparar a Instalação

O BitDefender analisa o seu sistema e verifica se há outro software de segurança instalado.

### Análise Rápida

É efectuada uma análise rápida às áreas críticas do seu sistema para garantir que não existe malware activo.

A análise não deverá demorar mais do que alguns minutos. Pode cancelá-la em qualquer momento clicando no respectivo botão.

**Importante**
É altamente recomendado que aguarde a conclusão da análise.
O malware activo pode interromper a instalação e causar a falha.

Depois de a análise terminar, os resultados são apresentados. Se for encontrada alguma ameaça, siga as instruções para a remover antes de continuar a instalação.

Clique em **Seguinte** para continuar.

### Remover Software de Segurança Existente

O BitDefender Antivirus Pro 2011 avisa-o se tiver outros produtos de segurança instalados no seu computador.Clique no botão respectivo para iniciar o processo de desinstalação e siga as instruções para remover os produtos detectados.

**Atenção**
É altamente recomendável que desinstale qualquer outro antivírus detectado antes de instalar BitDefender. Usar dois ou mais produtos antivírus ao mesmo tempo num computador pode bloquear totalmente o seu sistema.

Se o Windows Defender estiver activado, é recomendado que autorize o BitDefender a desactivá-lo.

Clique em **Seguinte** para continuar.

## 3.3. Passo 3 - Registo

O processo de registo do BitDefender consiste em registar o produto com uma chave de licença e activar os recursos em linha criando uma conta BitDefender.

### Registar o seu produto

Proceda consoante a sua situação:

- **Comprei o BitDefender Antivirus Pro 2011 num CD ou em linha**

  Neste caso, tem de registar o produto:

  1. Insira a chave de licença no campo de edição.

**Nota**
Pode encontrar a sua chave de licença:

- Na bolsa do CD.
- ou no cartão de registo do produto.
- no e-mail da sua compra on-line.

Se não possuir uma chave de licença BitDefender, clique no link que lhe facultamos para ir até à loja on-line do BitDefender e adquirir uma.

2. Clique em **Registar Agora**.
3. Clique **Seguinte**.

- **Transferi o BitDefender Antivirus Pro 2011 para avaliação**

  Neste caso, pode utilizar todos os recursos do programa durante 30 dias.Para iniciar o período de avaliação, seleccione **Quero avaliar o BitDefender Antivirus Pro 2011 durante 30 dias** e clique em **Seguinte**.

## Activar Recursos Online

TEM de criar uma conta BitDefender de forma a poder receber as actualizações do mesmo.A conta BitDefender também lhe dá acesso a suporte gratuito e a ofertas promocionais especiais.Se perder a sua chave de licença do BitDefender, pode entrar na sua conta em http://myaccount.bitdefender.com e recuperá-la.

Se não deseja criar uma conta BitDefender neste momento, seleccione **Criar Conta Mais Tarde** e clique em **Seguinte**.

Nota

Se estiver a instalar o BitDefender Antivirus Pro 2011 para avaliação, tem de criar uma conta BitDefender agora.

Se adquiriu o produto, tem de criar uma conta no prazo de 30 dias após a instalação.

De outra forma, actue de acordo com a sua presente situação:

- **Não tenho uma conta BitDefender**

  Para criar uma conta BitDefender com sucesso, siga estes passos:

  1. Seleccione **Criar uma nova conta**.
  2. Digite as informações solicitadas nos campos correspondentes.Os dados que nos fornecer serão mantidos confidenciais.
     - **Nome de utilizador** - insira o seu endereço electrónico.
     - **Palavra-passe** - insira uma palavra-passe para a sua conta BitDefender.A palavra-passe tem de ter entre 6 e 16 caracteres de tamanho.
     - **Re-inserir a palavra-passe** - inserir novamente a palavra-passe previamente definida.

       Não tem de escrever novamente a palavra-passe se seleccionar não ocultar a palavra-passe enquanto escreve.

Nota
Uma vez com a conta activada, poderá utilizar o endereço de e-mail fornecido e a palavra-passe para entrar na sua conta em http://myaccount.bitdefender.com.

3. Opcionalmente, a BitDefender pode informá-lo acerca de ofertas especiais e promoções usando o endereço de e-mail da sua conta.Clique em **Ver Opções de Contacto** e seleccione uma das opções disponíveis na janela que aparece.
   - **Envie-me todas as mensagens**
   - **Enviar mensagens importantes**
   - **Não me enviem quaisquer mensagens**
4. Clique em **Submeter**.
5. Clique em **Seguinte** para continuar.

Nota
Antes de usar a sua conta, tem de a activar.
Verifique o seu e-mail e siga as instrucções da mensagem de e-mail que o serviço de registo BitDefender lhe enviou.

- **Já tenho uma conta BitDefender**

O BitDefender detectará automaticamente se já registou previamente uma conta BitDefender no seu computador.Nesse caso, forneça a palavra-passe da sua conta e clique em **Submeter**.Clique em **Seguinte** para continuar.

Se já tiver uma conta activada mas o BitDefender não a detecta, siga estes passos para registar essa conta ao produto:

1. Seleccione **Entrar (Conta Existente)**.
2. Digite o endereço de e-mail e a palavra-passe da sua conta nos campos correspondentes.

Nota
Se não se lembra da sua palavra-passe, clique em **Esqueceu a sua palavra-passe?** e siga as instruções.

3. Opcionalmente, a BitDefender pode informá-lo acerca de ofertas especiais e promoções usando o endereço de e-mail da sua conta.Clique em **Ver Opções de Contacto** e seleccione uma das opções disponíveis na janela que aparece.
   - **Envie-me todas as mensagens**
   - **Enviar mensagens importantes**
   - **Não me enviem quaisquer mensagens**
4. Clique em **Submeter**.
5. Clique em **Seguinte** para continuar.

## 3.4. Passo 4 - Escolher o Modo

Aqui pode escolher o tipo de instalação a efectuar e o modo do interface a utilizar.

### Escolher o Tipo de Configuração

Estão disponíveis as seguintes opções de configuração:

- **Configuração Fácil** - seleccione esta opção se preferir uma instalação rápida e se não pretender configurar as definições do BitDefender em pormenor.
- **Configuração Personalizada** - seleccione esta opção se preferir personalizar a instalação e as definições do BitDefender.

Para ver um tutorial de ajuda com a instalação, clique em **Obter Ajuda**

Nota

Para instalar o BitDefender com uma configuração predefinida e avançar directamente para o último passo do assistente de instalação, seleccione **Saltar Configuração**.

Clique em **Seguinte** para continuar.

### Escolher Localização da Configuração

Nota

Este passo só aparece se tiver escolhido uma **Configuração Personalizada**.

Por defeito, BitDefender Antivirus Pro 2011 será instalado em `C:\Programas\BitDefender\`.Se deseja alterar este caminho de instalação, clique em **Explorar** e seleccione a pasta na qual pretende que o BitDefender seja instalado.

Pode partilhar os ficheiros e as assinaturas com outros utilizadores do BitDefender.Desta forma, as actualizações do BitDefender são mais rápidas.Se não quiser activar este recurso, seleccione a respectiva caixa.

Nota

Não será partilhada qualquer informação de identificação pessoal se este recurso estiver activado.

Clique em **Seguinte** para continuar.

### Escolher o Interface de Utilizador

Seleccione o modo do interface do utilizador que melhor se adequa às suas necessidades.BitDefender Antivirus Pro 2011 dá-lhe a possibilidade de escolher entre três interfaces, cada um concebido de acordo com as necessidades de diferentes utilizadores.

Modo Básico
: Indicado para principiantes em computadores e pessoas que querem que o BitDefender proteja o seu computador e dados sem incómodos. Este modo é simples de usar e requer a mínima interacção da sua parte.

  Tudo o que tem de fazer é reparar as incidências indicadas pelo BitDefender. Um assistente de passo-a-passo intuitivo ajudá-lo-á a resolver essas incidências.Adicionalmente, pode levar a cabo tarefas comuns, tais como actualizar as assinaturas de vírus e os ficheiros do BitDefender ou analisar o computador.

Modo Intermédio
: Pode configurar as definições principais do BitDefender, corrija os problemas separadamente, gira os produtos do BitDefender instalados nos computadores da sua rede e escolha os problemas a monitorizar.

Modo Avançado
: Adequado para os utilizadores com mais conhecimentos tecnicos, este modo permite-lhe configurar completamente cada funcionalidade do BitDefender.Também pode usar todas as tarefas disponiveis para proteger o seu computador e dados.

Faça a sua selecção e clique em **Seguinte** para continuar.

## 3.5. Passo 5 - Configurar

Aqui pode personalizar o seu produto.

### Configurar Definições

Nota
Este passo só aparece se tiver definido o **Modo Avançado** do BitDefender.

Aqui pode activar/desactivar os recursos do BitDefender, organizados em duas categorias.Para alterar o estado de uma definição, clique no respectivo interruptor.

- **Opções de Segurança**

  Aqui, pode activar ou desactivar configurações do produto que abrangem diversos aspectos da segurança do computador e dos dados.

| Definições | Descrição |
|---|---|
| **Antivírus** | A protecção em tempo-real assegura que todos os ficheiros acedidos por si ou por uma aplicação são analisados. |

| Definições | Descrição |
|---|---|
| **Actualização Automática** | A actualização automática assegura que os produtos e as assinaturas mais recentes da BitDefender são descarregados da Internet e instalados automaticamente numa base regular. |
| **Analisar Vulnerabilidades** | A Verificação Automática de Vulnerabilidades assegura que o software crucial no seu PC está actualizado. |
| **Antiphishing** | A protecção Antiphishing web em tempo-real detecta e alerta-o em tempo-real se uma página web está feita para roubar informação pessoal. |
| **Controlo de identidade** | O Controlo de Identidade ajuda a impedir que os seus dados pessoais sejam expostos na Internet sem o seu consentimento. Bloqueia todas as mensagens instantâneas, mensagens de e-mail ou outras formas de transmissão de dados pela web que tenha definido como sendo privado para destinatários não autorizados (endereços). |
| **Encriptação de Chat** | A Encriptação de Conversa através do Yahoo! Messenger e Windows Live Messenger só é possível se a pessoa de contacto utilizar um produto BitDefender compativel. |

- **Configuração Geral**

  Aqui, pode activar ou desactivar as definições referentes ao produto e à experiencia do utilizador.

| Definições | Descrição |
|---|---|
| **Modo de Jogo** | O Modo de Jogo modifica temporariamente as definições de segurança de forma a minimizar o seu impacto no desempenho do seu sistema durante o jogo. |
| **Detecção de Modo Portátil** | O Modo Portátil modifica temporariamente as definições de segurança de forma a minimizar o seu impacto sobre o tempo de vida da bateria do seu portátil. |
| **Definição de Palavra-passe** | Isto assegura que as definições do BitDefender só podem ser modificadas pela pessoa que conhece esta palavra-passe. |

| Definições | Descrição |
|---|---|
| | Quando activar esta opção, será solicitado a configurar as definições de palavra-passe.Insira a palavra-passe desejada nos dois campos e clique em **OK** para definir a palavra-passe. |
| **Notícias BitDefender** | Ao activar esta opção, irá receber notícias importantes sobre a empresa BitDefender, sobre as actualizações do produto ou sobre novas ameaças de segurança. |
| **Alertas de Notificação do Produto** | Ao activar esta opção, irá receber alertas de informação. |
| **Barra de Actividade da Análise** | A barra de actividade da análise é uma janela pequena, transparente, que indica o progresso da actividade da análise do BitDefender.Para mais informação, por favor consulte o *"Barra de Actividade da Análise"* (p. 19). |
| **Enviar relatórios de vírus** | Ao activar esta opção, os relatórios das análises são enviados para o Laboratório BitDefender para análise. Estes relatórios não contém qualquer informação considerada pessoal e confidencial (tal como o nome, endereço IP, etc) e não serão usados para qualquer propósito comercial. |
| **Detecção de Surtos** | Ao activar esta opção, os relatórios relativos a potenciais surtos de vírus são enviados para o Laboratório BitDefender para análise. Estes relatórios não contém qualquer informação considerada pessoal e confidencial (tal como o nome, endereço IP, etc) e não serão usados para qualquer propósito comercial. |

Clique em **Seguinte** para continuar.

## Configurar as Ferramentas

Nota
Este passo só aparece se tiver definido o **Modo Básico** or **Modo Intermédio** do BitDefender.

Com os **Meus Instrumentos**, pode personalizar o painel de instrumentos adicionando atalhos para os recursos que são mais importantes para si.Desta forma, pode garantir o fácil acesso a eles.

Neste ecrã, pode adicionar atalhos para qualquer um dos seguintes instrumentos:

- Modo Jogo - configure o BitDefender para impedir que este interfira com o seu jogo.
- Modo Portátil - modifica temporariamente as definições da protecção para minimizar o impacto na duração da bateria do seu portátil.
- Gestão da rede Doméstica - gere os produtos BitDefender instalados na rede doméstica a partir de um único computador.
- Análise Minuciosa ao Sistema - efectua um análise a todo o sistema.

Seleccione os instrumentos que pretende adicionar e clique em **Seguinte** para continuar.

### Gestão da Rede Pessoal

Nota

Este passo só aparece se tiver adicionado a Gestão de Rede Doméstica aos Meus Instrumentos.

Pode seleccionar uma das três opções:

- **Definir este PC como Servidor**

  Seleccione esta opção se pretende gerir os produtos BitDefender noutros computadores da rede doméstica a partir deste.

  É necessária uma palavra-passe para entrar na rede.Introduza nas respectivas caixas de texto e clique em **Submeter**.

- **Definir este PC como Cliente**

  Seleccione esta opção se o BitDefender será gerido a partir de outro computador da rede doméstica que também tem o BitDefender instalado.

  É necessária uma palavra-passe para entrar na rede.Introduza nas respectivas caixas de texto e clique em **Submeter**.

- **Saltar a configuração por agora**

  Seleccione esta opção para configurar este recurso mais tarde na janela do BitDefender.

Clique em **Seguinte** para continuar.

## 3.6. Passo 6 - Opções de Suporte

Aqui pode personalizar as opções de ajuda e suporte:

- Activar / desactivar as **Dicas Inteligentes**.As Dicas Inteligentes são mensagens personalizadas apresentadas no Painel de Instrumentos do BitDefender para o ajudar a melhorar o desempenho do seu computador.
- Confirme o endereço electrónico que irá utilizar se tiver de contactar o Apoio ao Cliente do BitDefender. Se não pretender contactar o Apoio ao Cliente por correio electrónico, seleccione a caixa respectiva.

## 3.7. Passo 7 - Confirmar

Aqui pode rever a configuração seleccionada.

Por defeito, também são agendadas duas tarefas:

- É agendada uma análise minuciosa ao sistema imediatamente após a conclusão da instalação.

  É recomendado que realize esta análise profunda para detectar todas as ameaças de malware presentes no seu sistema.

- Um análise ao sistema foi agendada para ser executada aos Domingos, às 2h.

  É vivamente recomendado que analise o seu sistema pelo menos uma vez por semana.Seleccione um dia e uma hora diferentes se a altura predefinida não for conveniente para si.Se o computador estiver desligado durante o momento do agendamento, a análise será levada a cabo da próxima vez que iniciar o seu computador.

Clique em **Terminar**.

## 3.8. Passo 8 - Terminar

A instalação está, agora, perto da conclusão. As definições finais são aplicadas e é efectuada uma actualização.

O assistente vai ser automaticamente encerrado no final da instalação.Se a opção foi seleccionada no passo anterior, será iniciada uma análise minuciosa ao sistema.

Nota
Poderá ser necessário reiniciar o sistema.

# 4. Fazer o Upgrade de Versões Anteriores do BitDefender

Pode fazer upgrade para o BitDefender Antivirus Pro 2011 se estiver a usar a versão beta, 2008, 2009 ou 2010 do BitDefender Antivirus Pro 2011.

Há duas formas de fazer o upgrade:

- Instalar o BitDefender Antivirus Pro 2011 directamente sobre a antiga versão.Se instalar directamente sobre a versão 2010, a Quarentena é automaticamente importada.
- Remova a anterior versão, reinicie o computador e instale a nova versão tal como descrito na secção "*Instalar BitDefender*" (p. 5).Não serão guardadas as definições do produto.Use este método de upgrade se outros falharem.

# 5. Remover ou Reparar o BitDefender

Se pretende reparar ou remover o BitDefender Antivirus Pro 2011, faça o seguinte a partir do menu Iniciar do Windows: **Iniciar** → **Todos os Programas** → **BitDefender 2011** → **Reparar ou Desinstalar**.

Vai aparecer um assistente para o ajudar a concluir a tarefa desejada.

1. **Reparar ou Remover**

   Seleccione a acção que quer efectuar:

   - **Reparar** - para reinstalar todos os componentes do programa.
   - **Remover** - para remover todos os componetes instalados.

   Nota

   Recomendamos que escolha **Desinstalar** para uma reinstalação limpa.

2. **Confirmar Acção**

   Leia atentamente a informação disponibilizada antes de clicar em **Seguinte** para confirmar a acção.

3. **Progresso**

   Aguarde que o BitDefender conclua a acção que seleccionou.Isto irá demorar vários minutos.

4. **Terminar**

   Os resultados são apresentados.

   Tem de reiniciar o computador para concluir o processo. Clique em **Reiniciar** para reiniciar imediatamente o seu computador ou em **Concluir** para fechar a janela e reiniciar mais tarde.

# Introdução

# 6. Apresentação

Assim que instalar o BitDefender Antivirus Pro 2011, o seu computador ficará protegido contra todos os tipos de malware (tais como vírus, spyware e cavalos de tróia).

Não é necessário configurar outras definições do BitDefender para além daquelas configuradas durante a instalação.No entanto, poderá querer usufruir das definições do BitDefender para optimizar e melhorar a sua protecção.

De vez em quando, deve abrir o BitDefender e corrigir as incidências existentes.Poderá ter que configurar componentes específicos do BitDefender ou levar a cabo acções preventivas para proteger o seu computador e os seus dados.Se desejar, pode configurar o BitDefender para não o alertar acerca de determinadas incidências.

Se não registou o produto (e não criou uma conta BitDefender), lembre-se de fazer isso antes que o período de testes termine.Tem de criar obrigatoriamente uma conta até 15 dias após instalar o BitDefender (se o registar com uma chave de licença, a data limite aumenta para 30 dias).De outra forma, o BitDefender deixa de ser actualizado.Para mais informaçãoon sobre o processo de registo, por favor consulte o "*Registo e a Minha Conta*" (p. 47).

## 6.1. A abrir o BitDefender

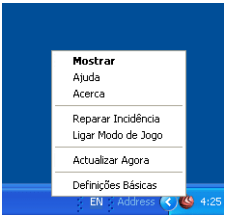
Para aceder ao interface principal do BitDefender Antivirus Pro 2011, utilize o menu Iniciar do Windows, seguindo o caminho **Iniciar → Todos os Programas → BitDefender 2011 → BitDefender Antivirus Pro 2011** ou, mais rapidamente, faça duplo-clique no ícone do BitDefender que está na área de notificação.

Para mais informações sobre a janela principal da aplicação, por favor consulte "*Janela Principal da Aplicação*" (p. 23).

## 6.2. Icon da Barra de Tarefas

Para gerir todo o produto mais rapidamente, pode usar o ícone da BitDefender que se encontra na barra de tarefas.Se fizer duplo-clique neste ícone, o BitDefender irá abrir. Também clicando com o botão direito do rato sobre ele aparecerá um menu contextual que lhe permitirá uma administração rápida do BitDefender.

- **Mostrar** - abre o interface principal do BitDefender.
- **Ajuda** - abre o ficheiro de Ajuda, que explica em detalhe como configurar e usar o BitDefender Antivirus Pro 2011.
- **Acerca** - abre uma janela onde pode ver informação acerca do BitDefender e onde procurar ajuda caso algo de inesperado lhe apareça.
- **Reparar todos incidências** - ajuda-o a remover as vulnerabilidades de segurança.Se a opção não está disponível, é porque não há incidências a reparar.Para mais informações, por favor consulte "*Reparar Incidência*" (p. 38).



Ícone Tray

- **Ligar/Desligar Modo de Jogo** - activa / desactiva Modo de Jogo.
- **Actualizar agora** - executa uma actualização imediata.Surge uma nova janela, onde pode ver o estado da actualização.
- **Preferências** - abre uma janela onde pode activar ou desactivas as principais definições do produto e reconfigurar o seu perfil de utilizador.Para mais informação, por favor consulte o "*Configurar Definições Principais*" (p. 41).

O ícone do BitDefender na area de notificação do sistema, informa quando ha incidências a afectar o seu computador ou a forma como o produto funciona, exibindo um símbolo especial, como o que se segue:

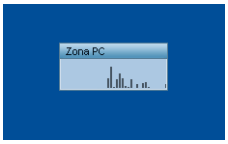
**Triângulo vermelho com um ponto de exclamação:** Questões críticas afectam a segurança do seu sistema. Eles requerem a sua atenção máxima e devem ser corrigidos o mais rapidamente possível.
**Letra G:**O produto funciona em Modo de Jogo.

Se o BitDefender não estiver a funcionar, o ícone da area de notificação do sistema fica com a cor cinzenta .Isto normalmente acontece quando a licença de chave expira. Também pode ocorrer quando os serviços da BitDefender não estão a responder ou quando outros erros afectam a actuação normal da BitDefender.

## 6.3. Barra de Actividade da Análise

A **Barra de Actividade da Análise** é um gráfico de visualização da actividade de verificação no seu sistema.Esta pequena janela, por defeito, está apenas disponível no Modo Avançado.

As barras cinzentas (a **zona PC**) mostram o número de ficheiros analisados por segundo, numa escala de 0 a 50.



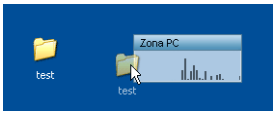

Barra de Actividade da Análise

**Nota**
A Barra de Actividade da Análise irá avisá-lo quando a protecção em tempo-real está desactivada ao mostrar-lhe uma cruz vermelha sobre a **Zona PC**).

## 6.3.1. Analisar Ficheiros e Pastas

Pode usar a barra de actividade da análise para analisar rapidamente ficheiros e pastas.Arraste o ficheiro ou a pasta que pretende analisar e deixe-a cair em cima da **Barra de Actividade da Análise**, como apresentado abaixo.

Arraste o ficheiro




Deixe cair o ficheiro

O Assistente de Análise Antivírus irá surgir e guiá-lo através do processo de análise.

**Opções de Análise.** As opções de análise estão pré-configuradas para obter os melhores resultados de detecção.Se forem detectados ficheiros infectados, o BitDefender irá tentar desinfectá-los (remover o código de malware). Se a desinfecção falha, o assistente de análise antivírus irá permitir-lhe definir outras acções a serem levadas a cabo sobre os ficheiros infectados.As opções de análise são padronizadas e não as pode alterar.

## 6.3.2. Desactivar/Restaurar Barra de Actividade da Análise

Quando não quiser ver o gráfico de visualização,clique apenas no botão direito e escolha **Esconder**.Para restaurar a barra de actividade da análise, siga os seguintes passos:

1. Abrir o BitDefender.

2. Clique no botão **Opções** no canto superior direito da janela e seleccione **Preferências**.
3. Na categoria Definições Gerais, seleccione a caixa correspondente a **Barra de Actividade da Análise** para a activar.
4. Clique em **OK** para salvar e aplicar as alterações.

## 6.4. Detecção Automática de Dispositivos

O BitDefender detecta automaticamente quando um dispositivo de armazenamento amovível se liga ao computador, e oferece-se para fazer um scan antes de você aceder aos arquivos.Isto é recomendado para prevenir que virus e malware infectem o seu computador.

Os dispositivos detectados encaixam-se numa destas categorias:

- CDs/DVDs
- Dispositivos de armazenamento USB, tais como pens e discos rígidos externos
- Unidades de Rede Mapeadas (remotas)

Quando dispositivos como estes são detectados, aparece uma janela de alerta.

Para analizar o dispositivo de armazenamento, clique em **Analizar**.O Assistente de Análise Antivírus irá surgir e guiá-lo através do processo de análise.

Se não quiser fazer o scan ao dispositivo, deve clicar **Não**. Nesse caso, uma destas opções podem ser úteis:

- **Não me perguntem novamente acerca deste tipo de dispositivo** - BitDefender não irá mais sugerir que analise dispositivos de armazenagem deste tipo quando eles estiverem ligados ao seu computador.
- **Desactivar detecção automática de dispositivos** - Não será mais solicitado para analisar novos dispositivos de armazenagem quando eles estiverem ligados ao computador.

Se acidentalmente desactivar a detecção automática de dispositivos e pretender activar, ou se deseja configurar as suas definições, siga estes passos:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Antivirus>Análise Virus**.
3. Na lista de tarefas de análise, localize a tarefa **Análise de Dispositivos**.
4. Clique com o botão direito do rato na tabela e seleccione **Propriedades**.Uma nova janela irá aparecer.
5. Na barra **Visão Geral** e configure as opções de análise como desejar.Para mais informação, por favor consulte o “*Configurar Definições da Análise*” (p. 71).

6. No separador **Detecção**, escolha quais os tipos de dispositivos de armanesamento a ser detectados.
7. Clique em **OK** para salvar e aplicar as alterações.

# 7. Janela Principal da Aplicação

O BitDefender Antivirus Pro 2011 vai de encontro às necessidades quer dos principiantes quer dos utilizadores mais técnicos. Assim, o interface gráfico do utilizador foi desenhado para servir quer uns quer outros.

Pode optar por ver o interface do utilizador em qualquer dos três modos, dependendo do seu computador e sobre a experiência anterior com o BitDefender.

Modo Básico

Indicado para iniciantes em computadores e pessoas que querem que o BitDefender proteja o seu computador e dados sem incomodos. Este modo é simples de usar e requer a minima interacção da sua parte.

Tudo o que tem de fazer é reparar as incidências indicadas pelo BitDefender. Um assistente de passo-a-passo intuitivo ajudá-lo-á a resolver essas incidências.Adicionalmente, pode levar a cabo tarefas comuns, tais como actualizar as assinaturas de vírus e os ficheiros do BitDefender ou analisar o computador.

Modo Intermédio

Destinado a utilizadores com alguns conhecimentos informática, este interface estende o que pode fazer em Modo Básico.

Pode corrigir problemas separadamente e escolher quais as questões a serem monitorizadas.Além disso, pode gerir remotamente os produtos BitDefender instalados nos computadores de sua casa.

Modo Avançado

Adequado para os utilizadores com mais conhecimentos tecnicos, este modo permite-lhe configurar completamente cada funcionalidade do BitDefender.Também pode usar todas as tarefas disponiveis para proteger o seu computador e dados.

O modo de visualização é seleccionado durante a instalação.

Para alterar op modo de visualização:

1. Abrir o BitDefender.
2. Clique no botão **Opções** que se encontra no canto superior direito da janela.
3. Seleccione o modo de visualização pretendido no menu.

## 7.1. Modo Básico

Se é um principiante em informática, o interface do Modo Básico pode ser a escolha mais adequada para si.Este modo é simples de usar e requer a mínima interacção da sua parte.

A janela está organizada em três áreas principais:

Área de Estado
A informação do estado é apresentada no lado esquerdo da janela.

Área Proteja o seu PC
Aqui pode tomar as acções necessárias para gerir a sua protecção.

Área de Ajuda
Aqui pode ficar a saber como utilizar o BitDefender Antivirus Pro 2011 e obter ajuda.

O botão **Opções** no canto superior direito da janela permite-lhe alterar o modo do interface e configurar as definições principais do programa.

No canto inferior direito da janela, pode encontrar vários links úteis.

| Link | Descrição |
|---|---|
| **Informação da Licença** | Abre uma janela onde pode ver a informação da chave de licença actual e registar o seu produto com a nova chave de licença. |
| Histórico | Permite-lhe ver um histórico detalhado de todas as tarefas levadas a cabo pelo BitDefender no seu sistema. |
| **Ajuda e Suporte** | Clique nesta hiperligação se precisar de ajuda com o BitDefender. |
| ? | Dá-lhe acesso ao ficheiro de ajuda que lhe mostra como usar o BitDefender. |

### 7.1.1. Estado da Área

A informação do estado é apresentada no lado esquerdo da janela.

- **Estado** - Alerta-o se incidências afectarem o seu computador e ajuda-o a repará-las.Ao clicar em **Reparar Incidências**, o assistente irá ajuda-lo a remover facilmente quaisquer ameaça do seu computador e segurança de dados.Para mais informações, por favor consulte “*Reparar Incidência*” (p. 38).
- **Estado da Licença** mostra quantos dias faltam até à licença expirar.Se estiver a utilizar uma versão de avaliação lou se a sua licença estiver a expirar, pode clicar em **Comprar Agora** para adquirir uma chave de licença.Para mais informações, por favor consulte “*Registo e a Minha Conta*” (p. 47).

### 7.1.2. Área Proteja o seu PC

Aqui pode tomar as acções necessárias para gerir a sua protecção.

Estão disponíveis três botões:

- **Segurança** disponibiliza os atalhos para as tarefas e definições de segurança.

- **Actualizar Agora** ajuda-o a actualizar as assinaturas de vírus e os ficheiros do BitDefender.Surge uma nova janela, onde pode ver o estado da actualização.Se as actualizações são detectadas, são automaticamente descarregadas e instaladas no seu computador.
- **Meus Instrumentos** permite-lhe criar atalhos para as suas tarefas e definições favoritas.

Para efectuar uma tarefa ou configurar definições, clique no respectivo botão e escolha o instrumento pretendido no menu.Para adicionar ou remover atalhos, clique no respectivo botão e escolha **Mais Opções**.Para mais informações, por favor consulte "*Ferramentas*" (p. 30).

### 7.1.3. Área de Ajuda

Aqui pode ficar a saber como utilizar o BitDefender Antivirus Pro 2011 e obter ajuda.

**Dicas Inteligentes** são uma forma fácil e divertida de aprender as melhores práticas para proteger o seu PC e como utilizar o BitDefender Antivirus Pro 2011.

Se precisar de ajuda, escreva uma palavra-chave ou uma pergunta no campo **Ajuda e Suporte** e clique em **Procurar**.

## 7.2. Modo Intermédio

Destinado a utilizadores com conhecimentos médios de informática, o Modo Intermédio é um interface simples que lhe dá acesso a todos os módulos num nível básico. Terá de acompanhar as advertências e alertas críticos e corrigir problemas indesejáveis.

A janela do Modo Intermédio está organizada em vários separadores.

Painel
: O painel ajuda-o a monitorizar e gerir facilmente a sua protecção.

Segurança
: Mostra o estado das definições de segurança e ajuda a corrigir os problemas detectados.Pode executar tarefas de segurança ou configurar definições de segurança.

REDE
: Mosta a estrutura da rede pessoal BitDefender.Aqui é onde pode levar a cabo diversas acção para configurar os produtos BitDefender instalados na sua rede pessoal.Desta forma, pode gerir a segurança da sua rede pessoal, a partir de um só computador.

O botão **Opções** no canto superior direito da janela permite-lhe alterar o modo do interface e configurar as definições principais do programa.

No canto inferior direito da janela, pode encontrar vários links úteis.

| Link | Descrição |
|---|---|
| **Informação da Licença** | Abre uma janela onde pode ver a informação da chave de licença actual e registar o seu produto com a nova chave de licença. |
| Histórico | Permite-lhe ver um histórico detalhado de todas as tarefas levadas a cabo pelo BitDefender no seu sistema. |
| **Comprar/Renovar** | Ajuda-o a adquirir uma chave de licença para o seu produto BitDefender Antivirus Pro 2011. |
| **Ajuda e Suporte** | Clique nesta hiperligação se precisar de ajuda com o BitDefender. |
| | Dá-lhe acesso ao ficheiro de ajuda que lhe mostra como usar o BitDefender. |

### 7.2.1. Painel

O painel ajuda-o a monitorizar e gerir facilmente a sua protecção.

O painel é composto de várias secções:

- **Detalhes do Estado** indica o estado de cada módulo principal usando frases explícitas e um dos seguintes ícones:

  **Círculo verde com uma marca de verificação:** Nenhuma incidências a afectar o estado de segurança.O seu computador e os seus dados estão protegidos.

  **Circulo vermelho com um ponto de exclamação:** Há incidências a afectarem a segurança do seu sistema.Incidências criticas requerem a sua atenção imediata. Incidências que não sejam críticas também deverão ser abordadas com a maior brevidade possível

  **Círculo cinzento com um ponto de exclamação:** A actividade dos componentes deste módulo não estão a ser monotorizados. Assim, não há informação disponível sobre o estado de segurança.Não há incidências específicas relativamente a este módulo.

  Clique no nome de um módulo para ver mais detalhes acerca do seu estado e para configurar o estado da monitorização dos seus componentes.

- **Estado da Licença** mostra quantos dias faltam até à licença expirar.Se estiver a utilizar uma versão de avaliação lou se a sua licença estiver a expirar, pode clicar em **Comprar Agora** para adquirir uma chave de licença.Para mais informações, por favor consulte “*Registo e a Minha Conta*” (p. 47).

- **Meus Instrumentos** permite-lhe criar atalhos para as suas tarefas e definições favoritas.Para mais informações, por favor consulte “*Ferramentas*” (p. 30).

- **Dicas Inteligentes** são uma forma fácil e divertida de aprender as melhores práticas para proteger o seu PC e como utilizar o BitDefender Antivirus Pro 2011.

## 7.2.2. Segurança

O separador Segurança permite-lhe gerir a segurança do seu computador e dos seus dados .

"Estado da Área" (p. 27)
"Tarefas Rápidas" (p. 27)

### Estado da Área

A área de estado é onde pode ver a lista completa de componentes de segurança monotorizados e o seu estado actual.Ao monotorizar cada módulo de segurança, o BitDefender irá informá-lo não só quando configurar definições que possam afectar a segurança do seu computador, mas também quando se esqueceu de realizar tarefas importantes.

O estado actual de um componente é indicado utilizando frases exclarecedoras e um dos seguintes ícones:

**Círculo verde com uma marca de verificação:** Não há incidências a infectarem o componente.
**Circulo vermelho com um ponto de exclamação:** Há incidências a infectarem o componente.

Apenas clique no botão **Corrigir** correspondendo à frase para corrigir a incidência reportada.Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

Para configurar os instrumentos a monitorizar:

1. Clique em **Adicionar/Editar Lista**.
2. Para activar ou desactivar a monitorização de um determinado item, utilize o respectivo botão.
3. Clique em **Fechar** para guardar as alterações e fechar a janela.

Importante
Para se certificar de que o seu sistema está completamente protegido, por favor permita a análise a todos os componentes e resolva todas as incidências reportadas.

### Tarefas Rápidas

Aqui pode encontrar links para as mais importantes tarefas de segurança:

- **Actualizar agora** - executa uma actualização imediata.

- **Análise Minuciosa ao Sistema** - inicia uma análise completa do seu computador (excepto arquivos). Para tarefas de análise a pedido adicionais clique na seta neste botão e seleccione uma tarefa de análise diferente.
- **Análise Personalizada** - abre um assistente que lhe permite criar e utilizar uma tarefa de análise personalizada.
- **Análise de Vulnerabilidade** - inicia um assistente que verifica o seu sistema em busca de vulnerabilidades e ajuda-o a repará-las.

### 7.2.3. REDE

Aqui é onde pode levar a cabo diversas acção para configurar os produtos BitDefender instalados na sua rede pessoal.Desta forma, pode gerir a segurança da sua rede pessoal, a partir de um só computador.

Para mais informações, por favor consulte "*A Sua Rede*" (p. 103).

## 7.3. Modo Avançado

O Modo Avançado dá-lhe acesso a cada componente específico do BitDefender. Aqui é onde pode configurar o BitDefender em detalhe.

Nota

O Modo Avançado é adequado para os utilizadores que têm conhecimentos informáticos acima da média, que conhecem o tipo de ameaças a que um computador está exposto e como funcionam os programas de segurança.

Do lado esquerdo da janela existe um menu que contém todos os módulos de segurança.Cada módulo possui um ou mais separadores onde pode configurar as respectivas definições de segurança ou executar tarefas de segurança e de administração.A lista seguinte descreve resumidamente cada módulo.Para mais informações, por favor consulte "Configuração e Gestão" (p. 51).

Geral
: Permite-lhe aceder às definições gerais ou ver o painel e a info detalhada do sistema.

Antivírus
: Permite-lhe configurar o escudo de vírus e as operações de análise em detalhe, definir excepções e configurar o módulo de quarentena.Aqui pode configurar a protecção antiphishing e o Consultor de Procura.

Controlo de Privacidade
: Permite-lhe evitar que sejam roubados dados do seu computador e protege a sua privacidade enquanto se encontra on-line.

Vulnerabilidade
: Permite-lhe manter o software crucial para o seu PC sempre actualizado.

Encriptação
Permite-lhe encriptar as comunicações via Yahoo e Windows Live (MSN) Messenger.

Modo Jogo/Portátil
Permite-lhe adiar as tarefas agendadas BitDefender enquanto o seu portátil está a funcionar a bateria e também elimina alertas e pop-ups enquanto está a jogar.

A Sua Rede
Permite-lhe configurar e gerir vários computadores do seu lar.

Actualização
Permite-lhe obter info das últimas actualizações, actualizar o produto e configurar o processo de actualização em detalhe.

**Registo**
Permite-lhe registar o BitDefender Antivirus Pro 2011, mudar a chave de licença ou criar uma conta BitDefender.

O botão **Opções** no canto superior direito da janela permite-lhe alterar o modo do interface e configurar as definições principais do programa.

No canto inferior direito da janela, pode encontrar vários links úteis.

| Link | Descrição |
|---|---|
| **Informação da Licença** | Abre uma janela onde pode ver a informação da chave de licença actual e registar o seu produto com a nova chave de licença. |
| Histórico | Permite-lhe ver um histórico detalhado de todas as tarefas levadas a cabo pelo BitDefender no seu sistema. |
| **Comprar/Renovar** | Ajuda-o a adquirir uma chave de licença para o seu produto BitDefender Antivirus Pro 2011. |
| **Ajuda e Suporte** | Clique nesta hiperligação se precisar de ajuda com o BitDefender. |
| ? | Dá-lhe acesso ao ficheiro de ajuda que lhe mostra como usar o BitDefender. |

# 8. Ferramentas

No Modo Básico ou no modo Intermédio do BitDefender, pode personalizar o seu painel de instrumentos adicionado atalhos paras as tarefas e definições que são mais importantes para si.Desta forma, pode aceder rapidamente às funcionalidades que utiliza normalmente e às definições avançadas sem ter de mudar para um modo de utilizador mais avançado.

Consoante o modo do interface de utilizador, os atalhos adicionados aos Meus Instrumentos estão disponíveis da seguinte forma:

Modo Básico
: Na área Proteja o seu PC, clique em Meus Instrumentos.Irá aparecer um menu.Clique num atalho para executar o respectivo instrumento.

Modo Intermédio
: Os atalhos aparecem em Meus Instrumentos.Clique num atalho para executar o respectivo instrumento.

Para abrir a janela onde pode seleccionar os atalhos que irão aparecer nos Meus Instrumentos, proceda da seguinte forma:

Modo Básico
: Na área Proteja o Seu PC, clique em Meus Instrumentos e escolha **Mais Opções**.

Modo Intermédio
: Clique num dos botões em Meus Instrumentos ou na hiperligação **Configurar Meus Instrumentos**.

Utilize os botões para seleccionar os recursos a adicionar aos Meus Instrumentos.Pode seleccionar uma das seguintes categorias de instrumentos.

- **Tarefas de Análise**

  Adicione as tarefas que utiliza regularmente para analisar se há ameaças de segurança no seu sistema.

| Tarefa de Análise | Descrição |
|---|---|
| **Análise Minuciosa** | Analisa todo o sistema.Na configuração por defeito, faz uma nálise em busca de todo o tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros. |
| **Análise Completa** | Analisa todo o sistema, excepto arquivos.Na configuração por defeito, analisa todos os tipos de malware excepto rootkits. |
| **Análise Rápida** | A Análise Rápida utiliza a análise nas nuvens para detectar malware em execução no seu |

| Tarefa de Análise | Descrição |
|---|---|
| | sistema.Normalmente, a realização de uma Análise Rápida demora menos de um minuto e utiliza uma facção dos recursos do sistema necessários para uma análise de vírus normal. |
| **Análise Personalizada** | Inicia um assistente que lhe permite criar uma tarefa de análise personalizada. |
| **Analisar Os Meus Documentos** | Use esta tarefa para analisar pastas de utilizadores actuais: `Os Meus Documentos`, `Ambiente de Trabalho` e `StartUp`. Isto irá assegurar a segurança dos seus documentos, uma área de trabalho segura e aplicações limpas a serem executadas no arranque. |
| **Agendar as Minhas Análises** | Encaminha para a janela de definições do Antivírus, onde pode personalizar as tarefas de análise a pedido. |

Para mais informações sobre as tarefas de análise, consulte "*Gerir Tarefas de Análise Existentes*" (p. 68).

- **Definições**

  Adicione atalhos para as definições do BitDefender que pretende configurar:

| Definições | Descrição |
|---|---|
| **Definições do Antivírus** | Configure o módulo do Antivírus. Para mais informações, consulte "*Protecção Antivírus*" (p. 56). |
| **Modo de Jogo** | Active o Modo Jogo. Para mais informações, por favor consulte "*Modo de Jogo*" (p. 98). |
| **Modo Portátil** | Active o Modo Portátil. Para mais informações, por favor consulte "*Modo Portátil*" (p. 101). |
| **Actualizar Agora** | Active uma actualização do BitDefender. Para mais informações, por favor consulte "*Actualização*" (p. 107). |
| **Ver & Corrigir Todas as Incidências** | Abra um assistente que o irá ajudar a corrigir todas as incidências de segurança que estão a afectar o seu sistema. Para mais informações, por favor consulte "*Reparar Incidência*" (p. 38). |

- **Ajuda & Suporte**

Entre na secção de suporte. Para mais informações, por favor consulte “Contacte-nos Directamente Do Seu Produto BitDefender” (p. 140).

# 9. Alertas e Pop-ups

BitDefender utiliza pop-ups e alertas para informar sobre o funcionamento ou sobre eventos especiais que poderão interessar-lhe e perguntar o que fazer sempre que necessário.Este capítulo apresenta os pop-ups e alertas do BitDefender que poderão surgir.

Pop-ups são pequenas janelas que aparecem temporariamente no ecrã a informar sobre vários eventos do BitDefender, como análise do correio electrónico, um novo computador que iniciou sessão na rede sem fios, uma nova regra de firewall, etc.Quando aparecerem pop-ups, ser-lhe-á pedido que clique no botão **OK** ou numa hiperligação, nada mais.

Os alertas são janelas a pedir que indique uma acção ou a informar sobre algo muito importante (por exemplo, a detecção de um vírus).Para além das janelas de alerta, poderá receber mensagens electrónicas ou instantâneas ou alertas na página de Internet.

Os pop-ups e alertas BitDefender incluem:

- Alertas Antivírus
- Alertas do Controlo Activo de Vírus
- Alertas de Detecção de Dispositivo
- Páginas de Alerta Antiphishing
- Alertas do Controlo de Privacidade

## 9.1. Alertas Antivírus

BitDefender protege-o contra vários tipos de malware, como vírus, spyware ou rootkits.Ao detectar um vírus ou outro malware, o BitDefender aplica uma determinada acção sobre o ficheiro infectado e informa-o através de uma janela de alerta.

Pode ver o nome do vírus, o caminho para o ficheiro infectado e a acção aplicada pelo BitDefender.

Clique **OK** para fechar a janela.

Importante

Quando é detectado um vírus, a melhor opção é analisar a totalidade do sistema para garantir que não há mais vírus.Para mais informação, por favor consulte o "*Como Posso Analisar Ficheiros e Pastas?*" (p. 112).
Se o vírus não tiver sido bloqueado, por favor consulte "*Remover Malware do Sistema*" (p. 129).

## 9.2. Alertas do Controlo Activo de Vírus

O Controlo Activo de Vírus pode ser configurado para o alertar e pedir-lhe para agir sempre que uma aplicação tentar executar umas acção possivelmente maliciosa.

Se estiver a utilizar o Modo Básico ou o Modo Intermédio, um pop-up irá aparecer sempre que o Controlo de Vírus Activo bloquear uma aplicação potencialmente prejudicial.Se estiver a utilizar o Modo Avançado, ser-lhe-á pedida uma acção, através de uma janela de alerta, sempre que que uma aplicação apresentar um comportamento malicioso.

Se conhece e confia na aplicação detectada, clicque em **Permitir**.

Se deseja fechar imediatamente a aplicação, clique em **OK**.

Seleccione a caixa de selecção **Lembrar esta acção para esta aplicação** antes de fazer a sua escolha e o BitDefender tomará a mesma acção no futuro para a aplicação detectada.A regra que é então criada será listada na janela da configuração do Controlo Activo de Vírus.

## 9.3. Alertas de Detecção de Dispositivo

O BitDefender detecta automaticamente quando um dispositivo de armazenamento amovível se liga ao computador, e oferece-se para fazer um scan antes de você aceder aos arquivos.Isto é recomendado para prevenir que virus e malware infectem o seu computador.

Os dispositivos detectados encaixam-se numa destas categorias:

- CDs/DVDs
- Dispositivos de armazenamento USB, tais como pens e discos rígidos externos
- Unidades de Rede Mapeadas (remotas)

Quando dispositivos como estes são detectados, aparece uma janela de alerta.

Para analizar o dispositivo de armazenamento, clique em **Analizar**.O assistente do Scan de Antivirus irá aparecer e guiá-lo durante o processo.

Se não quiser fazer o scan ao dispositivo, deve clicar **Não**. Nesse caso, uma destas opções podem ser úteis:

- **Não me perguntem novamente acerca deste tipo de dispositivo** - BitDefender não irá mais sugerir que analise dispositivos de armazenagem deste tipo quando eles estiverem ligados ao seu computador.
- **Desactivar detecção automática de dispositivos** - Não será mais solicitado para analisar novos dispositivos de armazenagem quando eles estiverem ligados ao computador.

Se acidentalmente desactivar a detecção automática de dispositivos e pretender activar, ou se deseja configurar as suas definições, siga estes passos:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Antivirus>Análise Virus**.
3. Na lista de tarefas de análise, localize a tarefa **Análise de Dispositivos**.
4. Clique com o botão direito do rato na tabela e seleccione **Propriedades**.Uma nova janela irá aparecer.
5. Na barra **Visão Geral** e configure as opções de análise como desejar.Para mais informação, por favor consulte o "*Configurar Definições da Análise*" (p. 71).
6. No separador **Detecção**, escolha quais os tipos de dispositivos de armanesamento a ser detectados.
7. Clique em **OK** para salvar e aplicar as alterações.

## 9.4. Alertas Antiphishing

Com a protecção antiphishing activada, o BitDefender alerta quando tentar aceder a páginas da Internet que poderão roubar informações pessoais.Antes de poder aceder a uma página de Internet desse tipo, o BitDefender vai bloquear essa página e mostra um alerta genérico.

Verifique o endereço da página de Internet na barra de endereços do seu navegador.Procure pistas que poderão indicar que a página de Internet é utilizada para roubar a identidade.Se o endereço da página for suspeito, é recomendado que não o abra.

Aqui estão algumas dicas que poderá achar úteis:

- Se escreveu o endereço de um sítio de Internet legítimo, verifique se o endereço está correcto. Se estiver incorrecto, torne a escrever e navegue novamente para a página.
- Se clicar numa hiperligação de uma mensagem electrónica ou instantânea, verifique quem a enviou. Se o remetente for desconhecido, é provável que seja uma tentativa de phishing. Se conhecer o remetente, deve confirmar se essa pessoa enviou realmente a hiperligação.
- Se chegou à página ao navegar na Internet, consulte a página onde encontrou a hiperligação (clique no botão Retroceder do seu navegador).

Se quiser visualizar a página de Internet, clique na hiperligação correspondente para aplicar uma das seguintes acções:

- **Visualizar a página de Internet apenas desta vez.** Não há qualquer risco desde que não submeta informações na página de Internet.Se a página de Internet for legítima, pode adicioná-la à Lista Branca (clique na barra de ferramentas Antiphishing BitDefender e seleccione **Adicionar à Lista Branca**).

- **Adicionar a página de Internet à Lista Branca.** A página de Internet será apresentada imediatamente e o BitDefender não tornará a alertar sobre ela.

Importante

Adicione à Lista Branca apenas as páginas de Internet em que confia plenamente (por exemplo, o sítio do seu banco, lojas em linha conhecidas, etc.).O BitDefender não verifica a existência de phishing nas páginas de Internet da Lista Branca.

Pode gerir a protecção antiphishing e a Lista Branca com a barra de ferramentas do BitDefender no seu navegador de Internet.Para mais informação, por favor consulte o *"Gerir a Protecção Antiphishing do BitDefender no Internet Explorer e Firefox"* (p. 81).

## 9.5. Alertas do Controlo de Privacidade

O Controlo de Privacidade oferece aos utilizadores mais experientes alguns recursos adicionais para proteger a identidade.Será consultado sobre as acções a aplicar através de janelas de alerta específicas se escolher activar um dos seguintes componentes:

- O Controlo do Registo - irá pedir a sua permissão sempre que um programa tentar modificar uma entrada de registo de forma a poder ser executado durante o arranque do Windows.
- O Controlo de Cookies - irá pedir a sua permissão sempre que um novo site web tentar definir uma cookie.
- O Controlo de script - irá pedir a sua permissão sempre que um site web tente activar um script ou outro conteúdo activo.

### 9.5.1. Alertas de Registo

Se activar o Controlo de Registo, ser-lhe-á pedida permissão sempre que um programa tentar modificar uma entrada de registo de forma a poder ser executado durante o arranque do Windows.

Poderá ver o programa que está a tentar alterar o registo do Windows.

Nota

O BitDefender irá, normalmente, alertá-lo quando instalar novos programas que necessitem decorrer na próxima inicialização do seu computador. Na maioria dos casos, estes programas são legítimos e podem ser confiáveis.

Se não reconhece o programa e lhe parecer suspeito, clique em **Bloquear** para evitar que ele modifique o registo do Windows.De outra forma, clique em **Permitir** para permitir a modificação.

Baseado na sua resposta, a regra é criada e listada na tabela de regras.A mesma acção será aplicada sempre que este programa tentar modificar uma entrada no registo.

Para mais informação, por favor consulte o “*Controlo de registo*” (p. 89).

### 9.5.2. Alertas de Script

Se activar o Controlo de Scripts, ser-lhe-á pedida autorização sempre que um novo sítio de Internet tentar executar um script ou outro conteúdo activo.

Pode ver o nome do recurso.

clique em **Sim** ou **Não** e será criada, aplicada e listada uma regra na tabela das regras.A mesma acção será aplicada automaticamente sempre que o respectivo sítio de Internet tentar executar o conteúdo activo.

Nota
Algumas páginas de Internet poderão não ser correctamente visualizadas se bloquear o conteúdo activo.

Para mais informação, por favor consulte o “*Controlo de script* ” (p. 91).

### 9.5.3. Alertas de Cookie

Quando activado, o Controlo de Cookies vai pedir-lhe autorização sempre que um novo sítio de Internet tenta definir ou pedir um cookie.

Pode ver o nome da aplicação que está a tentar enviar um ficheiro de cookie.

clique em **Sim** ou **Não** e será criada, aplicada e listada uma regra na tabela das regras.A mesma acção será automaticamente aplicada sempre que efectuar a ligação ao respectivo sítio.

Para mais informação, por favor consulte o “*Controlo de cookies* ” (p. 90).

# 10. Reparar Incidência

O BitDefender utiliza um sistema de emissão de monitoramento para detectar e informá-lo sobre os problemas que podem afectar a segurança do seu computador e dos seus dados. Por defeito, ele irá acompanhar apenas algumas questões que são consideradas muito importantes. No entanto, pode sempre configurá-lo conforme necessário, escolhendo as questões específicas sobre que deseja ser notificado.

É assim que as questões pendentes são notificadas:

- É mostrado um símbolo especial sobre o ícone do BitDefender no tabuleiro de sistema a indicar incidências pendentes.Além disso, se mover o cursor do rato sobre o ícone, uma janela pop-up irá confirmar a existência de questões pendentes.
- Quando abre o BitDefender, a área de Estado da Segurança vai indicar o número de incidências que afectam o seu sistema.
  - No Modo Básico, o estado de segurança é apresentado no lado esquerdo da janela.
  - No Modo Avançado, vá a **Geral > Painel** para verificar o estado da segurança.

## 10.1. Assistente Reparar Incidências

A forma mais fácil de corrigir as incidências existentes é seguir o passo-a-passo o **assistente Reparar Incidências** .Para abrir o assistente, faça uma das seguintes coisas:

- Clique com o botão direito do rato no ícone do BitDefender na area de notificação e seleccione **Reparar Incidências**.
- Abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:
  - No Modo Básico, clique em **Ver Todas as Incidências**.
  - No Modo Avançado, vá a **Geral > Painel** e clique em **Ver Todas as Incidências**.

  Nota
  Também pode adicionar um atalho a Meus Instrumentos.

É apresentada uma lista das ameaças de segurança existentes no seu computador.

Todas as incidências estão seleccionadas para serem solucionadas. No caso de existir uma incidência que não quer resolver, escolha a caixa de selecção correspondente. Se o fizer, o estado mudará para **Saltar**.

Nota
Se não pretender ser notificado sobre determinadas incidências, tem de configurar o sistema de alerta, tal como descrito na secção seguinte.

Para resolver a incidência seleccionada, clique em **Iniciar**. Algumas incidências são tratadas imediatamente. Para outras, o assistente ajuda-o a resolvê-las.

A incidência que este assistente o ajuda a tratar pode ser agrupada numa destas categorias:

- **Desactivar definições de segurança.** Tais incidências são reparadas imediatamente, ao activar as respectivas definições de segurança.
- **Ferramentas preventivas de segurança que deve realizar.** Um exemplo dessa tarefa é a análise ao seu computador. É recomendado que faça uma análise ao seu computador pelo menos uma vez por semana. O BitDefender irá automaticamente fazê-lo por si na maioria dos casos. Contudo, se alterou o agendamento das análises ou se o agendamento não se completou, será notificado sobre essa incidência.

  Quando reparar a incidência, o assistente ajuda-o a completar com sucesso a tarefa.
- **Vulnerabilidades dos Sistema.** O BitDefender verifica automaticamente o seu sistema por vulnerabilidades e alerta-o sobre eles.As vulnerabilidades do sistema incluem:
  - Senhas fracas para as contas de utilizador do Windows.
  - Software desactualizado no seu computador
  - actualizações do Windows em falta.
  - As actualizações automáticas do Windows estão desativadas.

  Quando essas incidências estão a ser reparadas, o assistente de análise de vulnerabilidades é iniciado. Este assistente ajuda-o a reparar as vulnerabilidades de sistema detectadas.Para mais informação, por favor consulte o *"A analisar em busca de Vulnerabilidades"* (p. 93).

## 10.2. Configurar os Alertas de Estado

O sistema de alerta de estado é pré-configurado para monitorizar e alertar sobre as incidências mais importantes que poderão afectar a segurança do seu computador e dos seus dados.Para além das incidências monitoradas por defeito, existem outras incidências de que pode vir a ser informado.

Pode configurar o sistema de alerta para melhor responder às suas necessidades de segurança escolhendo as incidências específicas sobre as quais pretende receber informações.Pode fazer isto no Modo Intermédio ou no Modo Avançado.

- No Modo Intermédio, a o sistema de alerta pode ser configurado a partir de locais diferentes.Siga estes passos:
  1. Vá ao separador **Segurança**.
  2. Clique na hiperligação **Adicionar/Editar Lista** na área de Estado.
  3. Utilize o botão do item para alterar o respectivo estado de alerta.
- No Modo Avançado, o sistema de alerta pode ser configurado a partir de um local central.Siga estes passos:
  1. Vá a **Geral > Painel**.
  2. Clique em **Adicionar/Editar Alertas**.
  3. Utilize o botão do item para alterar o respectivo estado de alerta.

# 11. Configurar Definições Principais

Pode configurar as definições do produto (incluindo reconfigurar o perfil de utilizador) a partir da janela de Preferências. Para abri-la, faça uma das seguintes acções:

- Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Preferências**.
- Clique com o botão direito do rato no ícone do BitDefender no tabuleiro de sistema e seleccione **Preferências**.

Nota

Para configurar as definições do programa em detalhe, use o interface no Modo Avançado.Para mais informações, por favor consulte "Configuração e Gestão" (p. 51).

As definições estão organizadas por três categorias:

- Opções de Segurança
- Definições de Alertas
- Configuração Geral

Para activar ou desactivar uma definição, utilize o respectivo botão.

Para aplicar e salvar as alterações, clique em **OK**. Para fechar a janela e não salvar as alterações, clique em **Cancelar**.

A hiperligação **Reconfigurar Perfil** no canto superior direito da janela permite-lhe reconfigurar o perfil de utilização.Para mais informação, por favor consulte o "*Reconfigurar o Perfil de Utilização*" (p. 44).

## 11.1. Opções de Segurança

Aqui, pode activar ou desactivar configurações do produto que abrangem diversos aspectos da segurança do computador e dos dados.Para activar ou desactivar uma definição, utilize o respectivo botão.

Atenção

Tenha cuidado ao desactivar a protecção em tempo-real do antivírus ou a actualização automática.Desactivar estas opções pode comprometer a segurança do seu computador. Se realmente necessita de as desactivar, não se esqueça de as activar novamente o mais rapidamente possível.

Estas são as definições disponíveis:

Antivírus

A protecção em tempo-real assegura que todos os ficheiros acedidos por si ou por uma aplicação são analisados.

Actualização Automática

A actualização automática assegura que os produtos e as assinaturas mais recentes da BitDefender são descarregados da Internet e instalados automaticamente numa base regular.As actualizações estão predefinidas para ocorrerem de hora em hora.

Ver Vulnerabilidades

A Análise Automática de Vulnerabilidade alerta-o e ajuda-o a corrigir vulnerabilidades do seu sistema que poderão afectar a segurança. Estas vulnerabilidades incluem software desactualizado, palavras-passe das contas de utilizador fracas ou actualizações do Windows em falta.

Antiphishing

A protecção Antiphishing web em tempo-real detecta e alerta-o em tempo-real se uma página web está feita para roubar informação pessoal.

Consultor de Procura

O Consultor de Procura analisa as hiperligações dos resultados das suas pesquisas e indica quais são seguras e quais não são.

Controlo de identidade

O Controlo de Identidade ajuda a impedir que os seus dados pessoais sejam expostos na Internet sem o seu consentimento. Bloqueia todas as mensagens instantâneas, mensagens de e-mail ou outras formas de transmissão de dados pela web que tenha definido como sendo privado para destinatários não autorizados (endereços).

Encriptação de Chat

A Encriptação de Conversa através do Yahoo! Messenger e Windows Live Messenger só é possível se a pessoa de contacto utilizar um produto BitDefender compativel.

O estado de algumas destas definições podem ser monitorizadas pelo sistema de monitorização do BitDefender.Se desactivar a definição de monitorização, o BitDefender irá identicar como incidencia que necessita de der reparada.

Se não desejar que uma definição de monitorização que desactivou seja detectada como Incidência, tem de configurar o sistema de monitorização para tal. Pode fazê-lo no Modo Intermédio ou no Modo Avançado.Para mais informações, por favor consulte “*Configurar os Alertas de Estado*” (p. 39).

## 11.2. Definições de Alertas

Nesta área, pode desactivar os pop-ups e alertas do BitDefender.BitDefender utiliza alertas para pedir acções e pop-ups para informar sobre acções automaticamente aplicadas ou outros eventos.Para activar ou desactivar uma categoria de alertas, utilize o respectivo botão.

Importante
A maioria destes alertas e pop-ups devem ser activados para evitar potenciais problemas.

Estas são as definições disponíveis:

**Alertas Antivírus**
Os alertas antivírus notificam quando o BitDefender detecta e bloqueia um vírus.Quando é detectado um vírus, a melhor opção é analisar a totalidade do sistema para garantir que não há mais vírus.

**Pop-ups do Controlo Activo de Vírus**
Se estiver a utilizar o Modo Básico ou o Modo Intermédio, um pop-up irá aparecer sempre que o Controlo de Vírus Activo bloquear uma aplicação potencialmente prejudicial.Se estiver a utilizar o Modo Avançado, ser-lhe-á pedida uma acção, através de uma janela de alerta, sempre que que uma aplicação apresentar um comportamento malicioso.

**Analisar pop-ups de correio electrónico**
Estes pop-ups são mostrados para informar que o BitDefender está a analisar a presença de malware nas mensagens electrónicas.

**Alertas da gestão de Rede Pessoal**
Estes alertas informam o utilizador quando estão a ser efectuadas acções administrativas à distância.

**Alertas da Quarentena**
Os alertas de quarentena informam quando são eliminados ficheiros antigos da quarentena.

**Pop-us de Registo**
Os pop-ups de registo são utilizados para lembrar que tem de registar o BitDefender ou para informar que a chave de licença está quase a expirar ou já expirou.

## 11.3. Configuração Geral

Aqui, pode activar ou desactivar as definições referentes ao produto e à experiencia do utilizador.Para activar ou desactivar uma definição, utilize o respectivo botão.

Estas são as definições disponíveis:

Modo de Jogo
O Modo de Jogo modifica temporariamente as definições de segurança de forma a minimizar o seu impacto no desempenho do seu sistema durante o jogo.

Detecção de Modo Portátil
O Modo Portátil modifica temporariamente as definições de segurança de forma a minimizar o seu impacto sobre o tempo de vida da bateria do seu portátil.

**Definição de Palavra-passe**

Para impedir que outra pessoa altere as definições do BitDefender, pode protegê-las com uma palavra-passe.Quando activar esta opção, será solicitado a configurar as definições de palavra-passe.Insira a palavra-passe desejada nos dois campos e clique em **OK** para definir a palavra-passe.

**Notícias BitDefender**

Ao activar esta opção, irá receber notícias importantes sobre a empresa BitDefender, sobre as actualizações do produto ou sobre novas ameaças de segurança.

**Alertas de Notificação do Produto**

Ao activar esta opção, irá receber alertas de informação.

Barra de Actividade da Análise

A barra de actividade da análise é uma janela pequena, transparente, que indica o progresso da actividade da análise do BitDefender.

**Enviar relatórios de vírus**

Ao activar esta opção, os relatórios das análises são enviados para o Laboratório BitDefender para análise. Estes relatórios não contém qualquer informação considerada pessoal e confidencial (tal como o nome, endereço IP, etc) e não serão usados para qualquer propósito comercial.

**Detecção de Surtos**

Ao activar esta opção, os relatórios relativos a potenciais surtos de vírus são enviados para o Laboratório BitDefender para análise. Estes relatórios não contém qualquer informação considerada pessoal e confidencial (tal como o nome, endereço IP, etc) e não serão usados para qualquer propósito comercial.

## 11.4. Reconfigurar o Perfil de Utilização

Durante a instalação, poderá configurar um perfil de utilização.O perfil de utilização reflecte as principais actividades desenvolvidas no computador. Dependendo do perfil de utilização, a interface do produto é organizada para permitir o acesso fácil às suas ferramentas preferidas.

Para reconfigurar o perfil de utilização, clique em **Reconfigurar Perfil** e siga o assistente de configuração.Pode navegar pelo assistente utilizando os botões **Seguinte** e **Retroceder**.Para sair do assistente, clique em **Cancelar**.

1. **Escolha o seu Modo**

   Seleccione o modo de interface preferido.

2. **Configurar as Ferramentas**

   Se tiver seleccionado o Modo Básico ou o Modo Intermédio, escolha os recursos para os quais deseja criar atalhos no Painel de Instrumentos.

3. **Configurar Definições**

Se tiver seleccionado o Modo Avançado, configure as definições BitDefender consoante o necessário.Para activar ou desactivar uma definição, utilize o respectivo botão.

4. **Gestão da Rede Pessoal**

Nota

Este passo só aparece se tiver adicionado a Gestão de Rede Doméstica aos Meus Instrumentos.

Pode seleccionar uma das três opções:

- **Definir este PC como "Servidor"**

  Seleccione esta opção se pretende gerir os produtos BitDefender noutros computadores da rede doméstica a partir deste.

  É necessária uma palavra-passe para entrar na rede.Introduza nas respectivas caixas de texto e clique em **Submeter**.

- **Definir este PC como "Cliente"**

  Seleccione esta opção se o BitDefender será gerido a partir de outro computador da rede doméstica que também tem o BitDefender instalado.

  É necessária uma palavra-passe para entrar na rede.Introduza a palavra-passe nas respectivas caixas de texto e clique em **Submeter**.

- **Saltar a configuração por agora**

  Seleccione esta opção para configurar este recurso mais tarde na janela do BitDefender.

5. **Configuração Concluída**

   Clique em **Terminar**.

# 12. Histórico e Eventos

O link **Histórico** no fundo da janela principal do BitDefender abre uma outra janela com o histórico dos & eventos. Esta janela oferece uma visão geral dos eventos relacionados com a segurança.Por exemplo, pode facilmente verificar se a actualização foi executada com sucesso, se foi encontrado malware no seu computador, se as suas tarefas de backup se executaram sem erros, etc.

De forma a ajudá-lo a filtrar o histórico dos & eventos BitDefender, as seguintes categorias são apresentadas do lado esquerdo:

- **Painel**
- **Antivírus**
- **Controlo de Privacidade**
- **Vulnerabilidade**
- **Encriptação de Conversa**
- **Modo Jogo/Portátil**
- **A Sua Rede**
- **Actualização**
- **Registo**

Está disponível uma lista de eventos para cada categoria. Cada evento vem com a seguinte informação: uma breve descrição, a acção que o BitDefender tomou e quando aconteceu, e a data e hora em que ocorreu. Se deseja saber mais informação acerca de um evento em particular da lista, faça duplo clique sobre esse evento.

Clique em **Limpar Log** se deseja remover antigos logs ou **Actualizar** para se certificar que os logs mais recentes são mostrados.

# 13. Registo e a Minha Conta

O Registo é um processo de dois passos:

1. **Activação do produto (registo de uma conta BitDefender).** Deve de criar uma conta BitDefender de forma a receber actualizações e a ter acesso a suporte técnico gratuito.Se já tem uma conta BitDefender, registe o seu produto BitDefender nessa conta.O BitDefender irá avisá-lo que necessita de activar o seu produto e ajudá-lo-á a reparar essa incidência.

   Importante

   Tem de criar uma conta no prazo de 15 dias depois de instalar o BitDefender.De outra forma, o BitDefender deixa de ser actualizado.

2. **Registo com uma chave de licença.** A chave de licença especifica durante quanto tempo está autorizado a usar o produto.Assim que a chave de licença expira, o BitDefender pára de executar as suas funções e de proteger o seu computador.Deve de adquirir uma chave de licença ou renovar a sua licença uns dias antes da actual licença expirar.

Se adquiriu o BitDefender Antivirus Pro 2011 num CD/DVD ou em linha, foi-lhe pedido que registasse o seu produto com uma chave de licença durante a instalação.

Se transferiu o BitDefender Antivirus Pro 2011 para avaliação, tem de registar o produto com uma chave de licença para continuar a utilizá-lo após o período de avaliação de 30 dias.Durante o período de testes, o produto é 100% funcional e pode testá-lo de forma a ver se está de acordo com as suas expectativas.

## 13.1. Registar BitDefender Antivirus Pro 2011

Se quer registar o produto com uma chave de licença ou alterar a sua chave de licença actual, clique na hiperligação **Informação de Licença**, localizado no fundo da janela do BitDefender.Irá aparecer a janela de registo de produto .

Pode ver o estado do registo do BitDefender, a actual chave de licença e quantos dias faltam para a licença expirar.

Para registar BitDefender Antivirus Pro 2011:

1. Insira a chave de licença no campo de edição.

   Nota

   Pode encontrar a sua chave de licença:
   - Na bolsa do CD.
   - ou no cartão de registo do produto.
   - no e-mail da sua compra on-line.

   Se não possuir uma chave de licença BitDefender, clique na hiperligação disponibilizada para iniciar o assistente que o irá ajudar a adquirir uma.

2. Clique em **Registar Agora**.
3. Clique em **Terminar**.

## 13.2. A activar o BitDefender

Para activar o BitDefender, necessita de criar, ou entrar numa conta BitDefender.Se não registou uma conta BitDefender durante o assistente de instalação, pode fazê-lo da seguinte forma:

Modo Básico
: Clique em **Ver Todas as Incidências**.O assistente irá ajudá-lo a corrigir todas as incidências pendentes, incluindo a activação do produto.

Modo Intermédio
: Vá ao separador **Segurança** e clique no botão **Ver & Corrigir** relacionado com o problema de actualização do produto.Clique em **Iniciar** na janela do assistente para activar o produto.

Modo Avançado
: Vá a **Registo** e clique no botão **Activar Produto**.

Irá abrir a janela de registo de conta.Aqui pode criar ou entrar em uma conta Bitdefender para activar o produto.

Se não deseja criar uma conta BitDefender neste momento, seleccione **Criar Conta Mais Tarde** e clique em **Concluir**.De outra forma, actue de acordo com a sua presente situação:

- "Não tenho uma conta BitDefender" (p. 48).
- "Já tenho uma conta BitDefender" (p. 49).

Importante

Tem de criar uma conta no prazo de 15 dias depois de instalar o BitDefender.De outra forma, o BitDefender deixa de ser actualizado.

### Não tenho uma conta BitDefender

Para criar uma conta BitDefender com sucesso, siga estes passos:

1. Seleccione **Criar uma nova conta**.
2. Digite as informações solicitadas nos campos correspondentes.Os dados que nos fornecer serão mantidos confidenciais.
   - **Nome de utilizador** - insira o seu endereço electrónico.
   - **Palavra-passe** - insira uma palavra-passe para a sua conta BitDefender.A palavra-passe tem de ter entre 6 e 16 caracteres de tamanho.

- **Re-inserir a palavra-passe** - inserir novamente a palavra-passe previamente definida.

  Não tem de escrever novamente a palavra-passe se seleccionar não ocultar a palavra-passe enquanto escreve.

- **Dica da Palavra-Passe** - introduza uma palavra ou frase que ajude a relembrar a palavra-passe no caso de a esquecer.

Nota
Uma vez com a conta activada, poderá utilizar o endereço de e-mail fornecido e a palavra-passe para entrar na sua conta em http://myaccount.bitdefender.com.

3. Opcionalmente, a BitDefender pode informá-lo acerca de ofertas especiais e promoções usando o endereço de e-mail da sua conta.Clique em **Ver Opções de Contacto** e seleccione uma das opções disponíveis na janela que aparece.
   - **Envie-me todas as mensagens**
   - **Enviar mensagens importantes**
   - **Não me enviem quaisquer mensagens**
4. Clique em **Submeter**.
5. Clique em **Concluir** para fechar a janela.

Nota
Antes de usar a sua conta, tem de a activar.
Verifique o seu e-mail e siga as instrucções da mensagem de e-mail que o serviço de registo BitDefender lhe enviou.

## Já tenho uma conta BitDefender

O BitDefender detectará automaticamente se já registou previamente uma conta BitDefender no seu computador.Nesse caso, forneça a palavra-passe da sua conta e clique em **Submeter**.Clique em **Concluir** para fechar a janela.

Se já tiver uma conta activada mas o BitDefender não a detecta, siga estes passos para registar essa conta ao produto:

1. Seleccione **Entrar (Conta Existente)**.
2. Digite o endereço de e-mail e a palavra-passe da sua conta nos campos correspondentes.

Nota
Se não se lembra da sua palavra-passe, clique em **Esqueceu a sua palavra-passe?** e siga as instruções.

3. Opcionalmente, a BitDefender pode informá-lo acerca de ofertas especiais e promoções usando o endereço de e-mail da sua conta.Clique em **Ver Opções de Contacto** e seleccione uma das opções disponíveis na janela que aparece.
   - **Envie-me todas as mensagens**
   - **Enviar mensagens importantes**
   - **Não me enviem quaisquer mensagens**
4. Clique em **Submeter**.
5. Clique em **Concluir** para fechar a janela.

## 13.3. Adquirir ou Renovar Chaves de Licença

Se o período de testes vai terminar em breve, deve de adquirir uma chave de licença e registar o seu produto.

De igual modo, se a sua actual chave de licença vai expirar brevemente, deve renová-la.Como cliente BitDefender, você beneficia de um desconto quando renovar a sua licença BittDefender. Pode também mudar de versão do seu produto com um desconto especial ou mesmo inteiramente grátis.

Para iniciar um procedimento simples e seguro, com quatro passos, que irá permitir adquirir uma nova chave ou renovar uma já existente, abra o BitDefender no Modo Intermédio ou no Modo Avançado e clique na hiperligação **Comprar** / **Renovar** ao fundo da janela.

# Configuração e Gestão

# 14. Configuração Geral

O módulo Geral dá-lhe informação sobre a actividade do BitDefender e do sistema.Aqui é onde pode modificar o comportamento global do BitDefender.

Para configurar as definições gerais:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Geral > Definições**.

- **Activar protecção das configurações por palavra-passe** - activa a definição de uma palavra-passe de forma a proteger a configuração do BitDefender.

  Nota
  Se não for a única pessoa a utilizar este computador, recomendamos que protega as suas configurações do BitDefender com uma palavra-passe.

  Introduza a palavra-passe no campo **Palavra-role="passe**, insira-a novamente no campo **Inserir de novo** e clique em **OK**.

  Uma vez que tenha definido a palavra-passe, será solicitado que a insira sempre que deseje alterar as configurações do BitDefender.Os outros administradores de sistema (se existirem) também terão de inserir a palavra-passe se desejarem alterar as configurações do BitDefender.

  Importante
  Se se esqueceu da palavra-passe, terá de reparar o produto para que possa modificar a configuração do BitDefender.

- **Mostrar Notícias BitDefender (notificações de segurança)** - mostra de tempos em tempos, notificações de segurança relacionadas com epidemias de vírus, enviadas pelo servidor do BitDefender.
- **Mostrar pop-ups (notas no ecrã)** - apresenta uma janela de pop-up no windows que mostra o estado do produto.Pode configurar o BitDefender para exibir pop-ups apenas quando o interface está no Modo Básico / Intermédio ou no Modo Avançado.
- **Mostra a barra de Actividade da Análise (gráfico no ecrã da actividade do produto)** - Exibe a barra de Actividade da Análisesempre que entrar no Windows.Limpe esta caixa se deseja que a barra de Actividade da Análise não seja mostrada daí em diante.

  Nota
  Esta opção pode ser configurada apenas para a actual conta de utilizador Windows.A barra de actividade da análise só está disponível no Modo Avançado.

## Configuração do Relatório de Vírus

- **Enviar relatórios de vírus** - envia relatórios que contêm vírus identificados no seu computador para os Laboratórios do BitDefender. Ajuda-nos a seguir o rasto das quebras dos vírus.

  Os relatórios não contêm dados confidenciais, tais como o seu nome, endereço de IP ou outros, e não serão usados com fins comerciais. A informação fornecida irá conter apenas o nome do vírus e será usada, somente para criar relatórios estatísticos.

- **Activar Detecção de Epidemias BitDefender** - envia relatórios para os Laboratórios do BitDefender com respeito a potenciais epidemias de vírus.

  Os relatórios não contêm dados confidenciais, tais como o seu nome, endereço de IP ou outros, e não serão usados para fins comerciais. A informação fornecida contém apenas o potencial vírus e será usada somente para ajudar a detectar novos vírus.

## Definições de Ligação

Vários componentes do BitDefender (os módulos de Firewall, LiveUpdate, Notificação de Vírus em Tempo Real e Notificação de Spam em Tempo Real) requerem acesso à Internet. O BitDefender possui um gestor de proxy que permite a configuração a partir de uma localização das definições de proxy utilizadas pelos componentes do BitDefender para aceder à Internet.

Se a sua empresa usa um servdior proxy para se ligar à Internet, deverá especificar as definições do proxy de forma a que o BitDefender se actualize sozinho. De outra forma, usará as definições do administrador que instalou o produto ou o utilizador actual por defeito do browser, caso haja algum.Para mais informação, por favor consulte o “*Como Posso Encontrar as Minhas Definições de Proxy?*” (p. 147).

Nota

As definições do proxy só podem ser configuradas por utilizadores com direitos administrativos no computador ou por power users (utilizadores que sabem a palavra-passe da configuração do produto).

Para gerir as definições proxy, clique em **Definições Proxy**.

Existem três categorias de definições de proxy:

- **Proxy detectado durante o Período de Instalação)** - as definições de proxy detectadas na conta de administrador durante a instalação e que podem ser configuradas apenas se estiver com sessão iniciada nessa conta. Se o servidor proxy requer um nome de utilizador e uma palavra-passe, deverá inseri-los nos campos correspondentes.

- **Browser por Defeito do Proxy** - as definições do proxy do actual utilizador, extraídas do browser por defeito. Se o servidor proxy requer um nome de utilizador e uma palavra-passe, deve de os inserir nos campos correspondentes.

  Nota
  Os browsers de internet suportados são o Internet Explorer, Mozilla Firefox e Opera. Se utiliza outro explorador por defeito, o BitDefender não será capaz de obter as definições do proxy do actual utilizador.

- **Personalizar Proxy** - definições de proxy que pode configurar se estiver logged in como administrador.

  As seguintes definições devem ser especificadas:
  - **Endereço** - introduza o IP do servidor proxy.
  - **Porta** - insira a porta que o BitDefender usa para se ligar ao servidor proxy.
  - **Nome de Utilizador** - introduza um nome de utilizador reconhecido pelo proxy.
  - **Palavra-passe** - introduza uma palavra-passe válida para o utilizador previamente definido.

O BitDefender utilizará os grupos de definições proxy na seguinte ordem até conseguir ligação à Internet:

1. as definições proxy especificadas.
2. as definições proxy detectadas no momento da instalação.
3. as definições proxy do actual utilizador.

Quando tentar ligar-se à Internet, cada conjunto de definições do proxy é experimentado na sua vez, até que o BitDefender se consiga ligar.

Primeiro, o conjunto que contém as suas definições do proxy será utilizado para ligar a Internet. Se esse não funcionar, as definições de proxy detectadas durante a instalação serão experimentadas logo a seguir. Finalmente se nenhuma dessa funcionar, as definições de proxy do utilizador actual serã retiradas do seu browser por defeito e usadas para obter a ligação à Internet.

Clique em **OK** para guardar as alterações e fechar a janela.

Clique em **Aplicar** para guardar as alterações, ou clique em **Defeito** para retornar às definições por defeito.

## Informação do Sistema

BitDefender permite-lhe visualizar, a partir de uma única localização, todas as configurações do sistema e as aplicações registadas para se executarem durante o iniciar do Windows. Desta forma, pode gerir a actividade da seu sistema e as aplicações instaladas nele como também identificar possíveis infecções.

Para obter a informação do sistema:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Geral > Informação do Sistema**.

A lista contém todos os itens carregados quando inicia o sistema assim como os itens carregados pelas diferentes aplicações.

Estão disponíveis três botões:

- **Restaurar** - muda a actual associação de ficheiros para o modo por defeito.Disponível apenas para as definições das **Associações de Ficheiros**!
- **Ir para** - abre uma janela onde o item seleccionado é colocado (o **Registo** por exemplo).

Nota
Dependendo do item seleccionado o botão **Ir Para** poderá não aparecer.

- **Actualizar** - reabre a secção de **Info Sistema**.

## Optimização

O separador Optimização é útil quando pretende efectuar uma análise a-pedido sem que o seu trabalho seja interrompido.

Por exemplo, se quiser efectuar uma Análise Minuciosa do Sistema, esta poderá demorar algum tempo se tiver muitos itens no seu disco rígido ou se a configuração do seu sistema não cumprir os requisitos recomendados.

Para aceder ao separador Optimização:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Geral > Optimização**.

A carga do sistema é constantemente monitorizada.Quando o sistema fica inactivo, o BitDefender pode executar:

- **Análise Minuciosa**
- **Análise Rápida**
- **Análise Completa**
- **Analisar Os Meus Documentos**

Nota
Seleccione a caixa **Actualizar o produto antes de executar esta tarefa** para garantir que possui as mais recentes definições antivírus.

# 15. Protecção Antivírus

BitDefender protege o seu computador de todo o tipo de malware (vírus, Trojans, spyware, rootkits e por aí fora).A protecção que BitDefender oferece está dividida em duas categorias:

- Protecção em Tempo-real - previne que novas ameaças de malware entrem no seu sistema.Poe exemplo, BitDefender irá analisar um documento word em busca de ameaças conhecidas quando você o abrir, e uma mensagem de e-mail quando recebe uma.

  A protecção em Tempo-real, também referida como análise no-acesso - os ficheiros são analisados à medida que os utilizadores lhes acedem.

  Importante
  Para prevenir que o seu computador seja infectado por vírus mantenha activa a **Protecção em Tempo-real**.

- Análise a-pedido - permite detectar e remover malware que já se encontra a residir no seu sistema.Esta é uma análise clássica iniciada pelo utilizador – você escolhe qual a drive, pasta ou ficheiro o BitDefender deverá analisar, e o mesmo é analisado – a-pedido.A tarefa de análise permite que crie rotinas personalizadas de análise e elas podem ser agendadas para serem executadas numa base regular.

Quando detecta um vírus ou outro malware, o BitDefender irá tentar remover automaticamente o código de malware do ficheiro e reconstruir o ficheiro original.Esta operação é designada por desinfecção.Os ficheiros que não podem ser desinfectados são movidos para a quarentena de modo a conter a infecção.Para mais informação, por favor consulte o "*Àrea de Quarentena*" (p. 78).

Se o seu computador estiver infectado com malware, por favor consulte "*Remover Malware do Sistema*" (p. 129).

Os utilizadores avançados podem configurar as exclusões da análise se não quiserem que certos ficheiros sejam analisados.Para mais informação, por favor consulte o "*Configurar Exclusões da Análise*" (p. 75).

## 15.1. Protecção em Tempo-real

O BitDefender providencia uma protecção contínua e em tempo-real, contra todo o tipo de ameaças de malware ao analisar os ficheiros acedidos, e as comunicações feitas através de aplicações de software de Mensagens Instantâneas (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

As predefinições da protecção em tempo real asseguram uma óptima protecção contra malware, com um impacto mínimo no desempenho do seu sistema.Pode alterar facilmente as definições da protecção em tempo real de acordo com as suas

necessidades mudando para um dos níveis de protecção predefinidos.Ou, no modo avançado, pode configurar as definições de análise em detalhe criando um nível de protecção personalizado.

Para saber mais, consulte os seguintes tópicos:

- "*Ajustar o Nível de Protecção em Tempo Real*" (p. 57)
- "*Criar um Nível de Protecção Personalizado*" (p. 58)
- "*Alterar as Acções Aplicadas aos Ficheiros Detectados*" (p. 59)
- "*Restaurar as Predefinições*" (p. 60)

Para proteger o seu sistema contra aplicações maliciosas desconhecidas, o BitDefender utiliza uma avançada tecnologia heurística (Controlo de Vírus Activo) e um Sistema de Detecção de Intrusão, que monitorizam constantemente o seu sistema.Para saber mais, consulte os seguintes tópicos:

- "*Configurar o Controlo Activo de Vírus*" (p. 61)
- "*Configurar o Sistema de Detecção de Intrusão:*" (p. 63)

### 15.1.1. Ajustar o Nível de Protecção em Tempo Real

O nível de protecção em tempo real determina as definições de análise da protecção em tempo real.Pode alterar facilmente as definições da protecção em tempo real de acordo com as suas necessidades mudando para um dos níveis de protecção predefinidos.

Para ajustar o nível de protecção em tempo real:

1. Abrir o BitDefender.
2. Dependendo do modo de interface do utilizador, proceda da seguinte forma:

   Modo Intermédio

   Abra o separador **Segurança** e clique em **Configurar o Antivírus**, nas Tarefas Rápidas, no lado esquerdo da janela.

   Abra o separador **Escudo**.

   Modo Avançado

   Vá a **Antivírus > Escudo**.

Nota

No Modo Básico e no Modo Intermédio, pode configurar um atalho para poder aceder a estas definições a partir do painel de instrumentos.Para mais informação, por favor consulte o "*Ferramentas*" (p. 30).

3. Arraste o cursor pela escala para definir o nível de protecção pretendido.Utilize a descrição do lado direito da escala para escolher o nível de protecção que melhor se adequa às suas necessidades de segurança.

### 15.1.2. Criar um Nível de Protecção Personalizado

Os utilizadores avançados poderão querer tirar partido das configurações de análise que o BitDefender oferece. O analisador pode ser configurado para evitar extensões de ficheiros, directorias ou arquivos que sabe serem inofensivos. Isto poderá reduzir o tempo de análise e melhorar a resposta do seu computador durante uma análise.

Pode configurar as definições da protecção em tempo real criando um nível de protecção personalizado.Para criar um nível de protecção personalizado:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Antivírus > Escudo**.
3. Clique em **Personalizar Nível**.
4. Configure as definições de análise como necessário.Para saber o que uma opção faz, mantenha o rato sobre a mesma e leia a descripção apresentada no fundo da janela.
5. Clique em **OK** para guardar as alterações e fechar a janela.

Poderá achar esta informação útil:

- Se não está familiarizado com alguns dos termos, procure-os no glossário.Pode também encontrar informação útil pesquisando a Internet.
- **Analisar ficheiros acedidos.** Pode definir o BitDefender para analisar todos os ficheiros acedidos, apenas aplicações (ficheiros de programa) ou tipos de ficheiro específicos que achar perigosos.A análise de todos os ficheiros acedidos proporciona uma maior segurança, enquanto a análise apenas das aplicações pode ser utilizada para melhorar o desempenho do sistema.

  As aplicações (ou ficheiros de programa) são muito mais vulneráveis a ataques de malware do que qualquer outro tipo de ficheiros.Esta categoria inclui as seguintes extensões de ficheiro:`.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml`; `.nws`.

  Se optar por **Analisar extensões definidas pelo utilizador**, é recomendado que inclua todas as extensões de aplicação para além das extensões de ficheiros que considere perigosas.

- **Analisar só ficheiros alterados.** Ao analisar apenas ficheiros novos e modificados, pode melhorar significativamente o desempenho do seu sistema sem comprometer a sua segurança.
- **Analisar dentro dos arquivos.** Analisar o interior de arquivos é um processo lento e que consome muitos recursos, não sendo, por isso recomendado para a protecção em tempo real.Os arquivos que contém ficheiros infectados não são uma ameaça imediata à segurança do seu sistema.O malware só pode afectar o seu sistema se o ficheiro infectado for extraído do arquivo e executado sem que a protecção em tempo real esteja activada.
- **Opções de acção.** Se pretender alterar as acções aplicadas a ficheiros detectados, procure dicas em *"Alterar as Acções Aplicadas aos Ficheiros Detectados"* (p. 59).
- **Opções de análise para tráfego de correio electrónico, Internet e mensagens instantâneas.** Para impedir que seja transferido malware para o seu computador, o BitDefender analisa automaticamente os seguintes pontos de entrada de malware:
  - correio recebido
  - tráfego da Internet
  - ficheiros recebidos através do Yahoo! Messenger e Windows Live Messenger

  Analisar o tráfego na Internet poderá abrandar um pouco a navegação, mas vai bloquear o malware proveniente da Internet, incluindo transferências "drive-by".

  Apesar de não ser recomendado, pode desactivar a análise ao correio electrónico, Internet ou mensagens instantâneas para aumentar o desempenho do sistema.Se desactivar as respectivas opções de análise, as mensagens electrónicas e os ficheiros recebidos e transferidos da Internet não serão analisados, permitindo que ficheiros infectados sejam guardados no seu computador.Esta é uma ameaça grave pois a protecção em tempo real vai bloquear o malware quando os ficheiros infectados forem acedidos (abertos, movidos, copiados ou executados).

### 15.1.3. Alterar as Acções Aplicadas aos Ficheiros Detectados

Os ficheiros detectados pela protecção em tempo real são agrupados em duas categorias:

- **Ficheiros infectados.** Os ficheiros detectados como infectados correspondem a uma assinatura de malware na Base de Dados de Assinaturas de Malware do BitDefender.Por norma, o BitDefender consegue remover o código de malware de um ficheiro infectado e reconstruir o ficheiro original. Esta operação é conhecida por desinfecção.

Nota

As assinaturas de malware são fragmentos de código extraídos de amostras de malware. São utilizados por programas antivírus para efectuar correspondência entre padrões e detectar malware.

A Base de Dados de Assinatura de Malware BitDefender é uma colecção de assinaturas de malware actualizada a toda hora pelos investigadores de malware da BitDefender.

- **Ficheiros suspeitos.** Os ficheiros são detectados como suspeitos pela análise heurística.Não foi possível desinfectar os ficheiros suspeitos por não estar disponível uma rotina de desinfecção.

Consoante o tipo do ficheiro detectado, são tomadas automaticamente as seguintes acções:

- Se for detectado um ficheiro infectado, o BitDefender tentará automaticamente desinfectá-lo.Se a desinfecção falhar, o ficheiro é movido para a quarentena de modo a restringir a infecção.

Importante

Para determinados tipos de malware, a desinfecção não é possível por o ficheiro detectado ser totalmente malicioso. Nestes casos, o ficheiro infectado é eliminado do disco.

- Se for detectado um ficheiro suspeito, o acesso a esse ficheiros será impedido para impedir uma potencial infecção.

Não deve alterar a acções predefinidas aplicadas aos ficheiros detectados excepto se tiver uma forte razão para isso.

Para alterar as acções predefinidas aplicadas aos ficheiros infectados ou suspeitos detectados:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Antivírus > Escudo**.
3. Clique em **Personalizar Nível**.
4. Configure as acções a aplicar em cada categoria de ficheiros detectados, consoante o necessário.A segunda acção é aplicada se a primeira falhar (por exemplo, se não for possível desinfectar, o ficheiro infectado é movido para a quarentena).

### 15.1.4. Restaurar as Predefinições

As predefinições da protecção em tempo real asseguram uma óptima protecção contra malware, com um impacto mínimo no desempenho do seu sistema.

Para restaurar as definições da protecção em tempo real:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.

2. Vá a **Antivírus > Escudo**.
3. Clique em **Nível Predefinido**.

## 15.1.5. Configurar o Controlo Activo de Vírus

O Controlo de Vírus Activo BitDefender detecta aplicações potencialmente destrutivas baseado no seu comportamento.

O Controlo de Vírus Activo monitoriza as aplicações executados no computador, procurando acções identificáveis como malware. Cada uma destas acções é classificada e é calculada uma pontuação geral para cada processo.Quando a pontuação geral de um processo atinge um determinado limite, o processo é considerado prejudicial. Consoante as definições do programa, o processo é automaticamente bloqueado ou poder ser-lhe pedido que indique a acção a aplicar.

O Controlo Activo de Vírus pode ser configurado para o alertar e pedir-lhe para agir sempre que uma aplicação tentar executar umas acção possivelmente maliciosa.

Se conhece e confia na aplicação detectada, clicque em **Permitir**.

Se deseja fechar imediatamente a aplicação, clique em **OK**.

Seleccione a caixa de selecção **Lembrar esta acção para esta aplicação** antes de fazer a sua escolha e o BitDefender tomará a mesma acção no futuro para a aplicação detectada.A regra que é então criada será listada na janela da configuração do Controlo Activo de Vírus.

Para configurar o Controlo Activo de Vírus:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Antivírus > Escudo**.
3. Clique em **Configuração Avançada**.
4. Abra o separador **AVC**.
5. Seleccione a marca da caixa correspondente para activar o Controlo Activo de Vírus.
6. Arraste o cursor pela escala para definir o nível de protecção pretendido.Utilize a descrição do lado direito da escala para escolher o nível de protecção que melhor se adequa às suas necessidades de segurança.

### Ajustar o Nível de Agressividade

Para configurar o nível de protecção do Controlo de Vírus Activo:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Antivírus > Escudo**.

3. Clique em **Configuração Avançada**.
4. Abra o separador **AVC**.
5. Arraste o cursor pela escala para definir o nível de protecção pretendido.Utilize a descrição do lado direito da escala para escolher o nível de protecção que melhor se adequa às suas necessidades de segurança.

## Configurar a Resposta a Comportamento Malicioso

Se uma aplicação apresentar um comportamento malicioso, ser-lhe-á perguntado se quer permitir ou bloquear.

Para configurar a resposta a comportamento malicioso:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Antivírus > Escudo**.
3. Clique em **Configuração Avançada**.
4. Abra o separador **AVC**.
5. Se quiser receber pedidos de acção quando o Controlo de Vírus Activo detecta uma aplicação potencialmente maliciosa, seleccione a caixa **Alertar-me antes de aplicar qualquer acção**.Para bloquear automaticamente uma aplicação que apresenta um comportamento malicioso (sem apresentar uma janela de alerta), desmarque esta caixa.

## Gerir a Lista de Aplicações Confiáveis/Não Confiáveis

Pode adicionar aplicações, que sabe que são fiáveis, à ista de aplicações fiáveis. Essas aplicação não serão mais analisadas pelo Controlo Activo de Vírus do BitDefender e será automaticamente permitido o acesso.

Para gerir as aplicações que não estão a ser monitorizadas pelo Controlo Activo de Vírus:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Antivírus > Escudo**.
3. Clique em **Configuração Avançada**.
4. Abra o separador **AVC**.
5. Clique no separador **Exclusões**.

As aplicações para as quais criou regras estão listadas na tabela **Exclusões**.O caminho para a aplicação e a acção que definiu para ela (Permitido ou Bloqueado) é exibido para cada regra.

Para alterar uma acção para uma aplicação, faça clique na actual acção e seleccione a outra acção a partir do menu.

Para gerir a lista, utiize os botões que se encontram por cima da tabela:

- **Adicionar** - adiciona uma nova aplicação à lista.
- **Remover** - remove uma aplicação da lista.
- **Editar** - Edita uma regra de uma aplicação.

### 15.1.6. Configurar o Sistema de Detecção de Intrusão:

O Sistema de Detecção de Intrusão BitDefender supervisiona as actividades da rede e do sistema à procura de comportamentos maliciosos ou violações de privacidade.

Para configurar o Sistema de Detecção de Intrusão:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Antivírus > Escudo**.
3. Clique em **Configuração Avançada**.
4. Abra o separador **IDS**.
5. Seleccione a caixa respectiva para activar o Sistema de Detecção de Intrusão.
6. Arraste o cursor pela escala para definir o nível de agressividade pretendido.Utilize a descrição do lado direito da escala para escolher o nível de agressividade que melhor se adequa às suas necessidades de segurança.

## 15.2. Análise a-pedido

O objectivo principal do BitDefender é manter o seu computador livre de vírus. Isto é inicialmente e essencialmente feito, mantendo novos vírus fora do seu computador e ao examinar as suas mensagens de e-mail e novos ficheiros descarregados ou copiados para o seu sistema.

Há o risco de o vírus já ter acedido ao seu sistema, antes mesmo de ter instalado o BitDefender. Este é o motivo, pelo qual é uma excelente ideia verificar vírus residentes no seu computador depois de instalar o BitDefender. E é defenitivamente uma boa ideia, a verificação frequente de vírus no seu computador.

A análise a-pedido está baseada em tarefas de análise. As tarefas de análise especificam as opções de análise e os objectos a serem analisados.Pode analisar o computador sempre que desejar ao executar as tarefas de análise por defeito ou as suas próprias tarefas de análise (tarefas definidas pelo utilizador). Pode também agendá-las para que se executem numa base regular ou quando o sistema está sem ser usado de forma a não interferir com o seu trabalho.Para instruções rápidas, por favor consulte os seguintes tópicos:

● *"Como Posso Analisar Ficheiros e Pastas?"* (p. 112)

- "*Como Posso Criar Uma Tarefa de Análise Personalizada?*" (p. 115)
- "*Como Posso Agendar uma Análise ao Computador?*" (p. 117)

### 15.2.1. Analisar Ficheiros e Pastas

Deve analisar os ficheiros e as pastas sempre que suspeitar de uma infecção.Clique com o botão direito do rato sobre o ficheiro ou pasta que pretende analisar e seleccione **Analisar com o BitDefender**.O Assistente de Análise Antivírus irá surgir e guiá-lo através do processo de análise.

Se quer analisar localizações específicas no seu computador, pode configurar e executar uma tarefa de análise personalizada.Para mais informação, por favor consulte o "*Como Posso Criar Uma Tarefa de Análise Personalizada?*" (p. 115).

Para analisar o seu computador ou parte dele pode usar as tarefas de análise por defeito ou pode criar as suas próprias tarefas de análise.Para executar uma tarefa de análise, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Básico
: Clique no botão **Segurança** e escolha uma das tarefas de análise disponíveis.

Modo Intermédio
: Vá ao separador **Segurança**.Clique em **Análise Minuciosa ao Sistema** na área de Tarefas Rápidas do lado esquerdo e escolha uma das tarefas de análise disponíveis.

Modo Avançado
: Vá a **Antivírus > Análise de Vírus**.Para levar a cabo uma tarefa de análise do sistema ou definida por si, clique no botão **Executar Tarefa** button.

Estas são as tarefas predefinidas que pode utilizar para analisar o seu computador:

**Análise Completa**
: Analisa todo o sistema, excepto arquivos.Na configuração por defeito, analisa todos os tipos de malware excepto rootkits.

**Análise Rápida**
: A Análise Rápida utiliza a análise nas nuvens para detectar malware em execução no seu sistema.Normalmente, a realização de uma Análise Rápida demora menos de um minuto e utiliza uma facção dos recursos do sistema necessários para uma análise de vírus normal.

**Análise Minuciosa**
: Analisa todo o sistema.Na configuração por defeito, faz uma nálise em busca de todo o tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.

Antes de inciar um processo de análise, deveria certificar-se que o BitDefender está actualizado com as assinaturas de malware mais recentes. Analisar o seu computador

usando assinaturas desactualizadas pode impedir que o BitDefender detecte novo malware encontrado desde a última actualização.

Para que o BitDefender possa efectuar uma verificação completa, tem de encerrar todos os programas abertos. É, especialmente, importante que encerre a sua conta de e-mail (por ex. Outlook, Outlook Express ou Eudora).

### Dicas de Análise

Eis aqui mais algumas dicas sobre a análise que lhe poderão ser úteis:

- Dependendo do tamanho do disco rígido, levar a cabo uma análise completa do seu computador (tal como uma Análise Minuciosa ou uma Análise Completa) pode levar algum tempo (uma hora ou mais).Logo, deve de levar a cabo essas análises em momentos em que não necessita do seu computador (por exemplo, durante a noite).

  Pode agendar a análise para começar quando for mais conveniente.Certifique-se de que deixa o seu computador ligado.Com o Windows Vista, certifique-se que o seu computador não está em Modo de Suspensão na altura para a qual a tarefa está agendada.

- Se descarrega frequentemente ficheiros da Internet para uma determinada pasta, crie uma nova tarefa de análise e defina essa pasta como alvo da análise.Agenda a tarefa para correr diariamente ou até com mais frequência.

- Existe um determinado tipo de malware que se prepara para ser executado durante o arranque do sistema ao alterar as definições do Windows.Para proteger o seu computador contra tal tipo de malware, pode agendar a tarefa de **Análise Autologon** para correr durante o iniciar do sistema.Tenha em atenção que a Análise Autologon pode afectar a performance do sistema durante um curto período de tempo após o iniciar do computador.

## 15.2.2. Assistente de Análise Antivírus

Sempre que inicie uma análise a-pedido (por exemplo, clicar botão direito sobre a pasta e selecionar **Analisar com BitDefender**), o assistente de análise antivírus BitDefender irá aparecer.Siga o processo guiado de três passos para completar o processo de análise.

Nota

Se o assistente de análise não surgir, a análise poderá estar configurada para correr silenciosamente, em segundo plano.Procure pelo ícone do progresso da análise na área de notificação.Pode clicar nesse icone para abrir a janela da análise e ver o seu progresso.

### Passo 1/3 - Analisar

BitDefender iniciará a análise dos objectos seleccionados.

Pode ver o estado da análise e as estatisticas (velocidade da análise, tempo decorrido, número de objectos analisados / infectados / suspeitos / ocultos e outras).

Espere que o BitDefender termine a análise.

Nota

O processo de análise pode demorar algum tempo, dependendo da complexidade da mesma.

**Arquivos protegidos com palavra-passe.** Quando é detectado um arquivo protegido por palavra-passe, dependendo das definições da análise, poderá ter de indicar a palavra-passe.Os arquivos protegidos por palavra-passe não podem ser analisados a não ser que forneça a palavra-passe.Estão disponíveis as seguintes opções:

- **Quero inserir a palavra-passe para este objecto.** Se quer que o BitDefender analise o arquivo, seleccione esta opção e insira a palavra-passe.Se não sabe a palavra-passe, escolha uma das outras opções.
- **Não quero inserir a palavra-passe para este objecto.** Seleccione esta opção para saltar a análise deste arquivo.
- **Não quero inserir a palavra-passe para nenhum objecto (saltar todos os objectos protegidos por palavra-passe).** Seleccione esta opção se não deseja ser incomodado acerca de arquivos protegidos por palavra-passe.O BitDefender não será capaz de os analisar, mas um registo dos mesmos será mantido no relatório da análise.

Clique em **OK** para continuar a analisar.

**Parar ou pausar a análise.** Pode parar o processo de análise a qualquer altura que desejar, fazendo clique em **Parar&**. Irá directamente para o último passo do assistente.Para parar temporariamente o processo de análise, clique em **Pausa**. Terá de clicar em**Retomar** para retomar a análise.

## Passo 2/3 - Seleccionar as acções

Quando a análise é completada, surge uma nova janela, onde pode ver os resultados da análise.

Se já não houver ameaças por resolver, clique em **Continuar**.Caso contrário, tem de configurar novas acções a aplicar a ameaças não resolvidas para proteger o seu sistema.

Os objectos infectados são apresentados em grupos, baseados no tipo de malware com que estão infectados.Clique no link correspondente a uma ameaça para descobrir mais informação acerca dos objectos infectados.

Pode escolher uma acção geral a ser levada a cabo para todas as incidências ou pode escolher acções separadas para cada grupo de incidências.Uma ou várias das seguintes opções poderão aparecer no menu:

**Não Tomar Acção**
Nenhuma acção será levada a cabo sobre os ficheiros detectados.Após a analisar terminar, pode abrir o relatório da análise para ver informação sobres esses ficheiros.

**Desinfectar**
Remove o código de malware dos ficheiros infectados.

**Apagar**
Remove os ficheiros detectados do disco.

**Mover para a quarentena**
Move os ficheiros infectados para a quarentena.O ficheiros em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece.Para mais informação, por favor consulte o "*Àrea de Quarentena*" (p. 78).

**Renomear ficheiros**
Altera o nome dos ficheiros ocultos ao acrescentar `.bd.ren` ao seu nome.Como resultado, será capaz de procurar e encontrar tais ficheiros no seu computador, se existirem.

Repare que este ficheiros ocultos, não são os ficheiros que esconde deliberadamente no Windows. Eles são ficheiros ocultos por programas especiais, conhecidos como rootkits.Os rootkits não são maliciosos por natureza, No entanto, eles são vulgarmente utilizados para tornar os vírus ou o spyware indetectáveis pelos programas antivírus.

Clique em **Continuar** para aplicar as acções especificadas.

## Passo 3/3 - Ver Resultados

Quando o BitDefender termina de reparar estas incidências, o resultado da análise aparecerá numa nova janela.Se deseja uma informação completa sobre o processo de análise, clique em **Mostrar Relatório** para ver o relatório da análise.

Importante
Se necessário, ser-lhe-á solicitado que reinicie o seu computador, para que o processo de limpeza seja completado.

Clique em **Fechar** para fechar a janela.

## BitDefender Não Pode Resolver Algumas Incidências

Na maioria dos casos o BitDefender desinfecta com sucesso o ficheiro infectado ou isola a infecção.No entanto, há incidências que não puderam ser automaticamente

resolvidas.Para mais informações e instruções sobre como remover manualmente o malware, por favor consulte “*Remover Malware do Sistema*” (p. 129).

BitDefender Detectou Ficheiros Suspeitos

Ficheiros suspeitos são ficheiros detectados pela análise heurística e que poderão estar infectados com malware cuja a assinatura de detecção ainda não foi disponibilizada.

Se foram detectados ficheiros suspeitos durante a análise, ser-lhe-á solicitado que os envie para o Laboratório do BitDefender.Clique **OK** para enviar estes ficheiros para análise no Laboratório do BitDefender.

## 15.2.3. Ver os Relatórios da Análise

Sempre que efectuar uma análise, é criado um relatório de análise.O relatório da análise contém informação detalhada acerca dos processos de análise registados, tal como as opções da análise, o alvo da análise, as ameaças encontradas e as acções tomadas sobre essas ameaças.

Pode abrir o relatório directamente no assistente de análise, assim que esta terminar, clicando em **Mostrar Relatório**.

Para consultar os relatórios de análise mais tarde:

1. Abrir o BitDefender.
2. Clique na hiperligação **Ver Relatórios** que se encontra no canto inferior direito da janela.
3. Clique em **Antivirus** do lado esquerdo do menu.
4. Na secção **Tarefas A Pedido**, pode ver as análises que foram recentemente efectuadas.Faça duplo clique nos eventos da lista para ver mais detalhes.Para abrir o relatório da análise, clique em **Ver Relatório de Análise**.O relatório da análise será aberto no seu explorador da internet.

Para eliminar uma entrada de registo, clique nela com o botão direito e seleccione **Eliminar**.

## 15.2.4. Gerir Tarefas de Análise Existentes

O BitDefender vem com diversas tarefas, criadas por defeito, que cobrem as incidências de segurança mais comuns. Pode também criar as suas próprias tarefas personalizadas.Para mais informação, por favor consulte o “*Como Posso Criar Uma Tarefa de Análise Personalizada?*” (p. 115).

Para gerir tarefas de análise existentes:

1. Abrir o BitDefender.
2. Dependendo do modo de interface do utilizador, proceda da seguinte forma:

Modo Intermédio

Abra o separador **Segurança** e clique em **Configurar o Antivírus**, nas Tarefas Rápidas, no lado esquerdo da janela.

Abra o separador **Análise de Vírus**.

Modo Avançado

Vá a **Antivírus > Análise de Vírus**.

Nota

No Modo Básico e no Modo Intermédio, pode configurar um atalho para poder aceder a estas definições a partir do painel de instrumentos.Para mais informação, por favor consulte o "*Ferramentas*" (p. 30).

Existem três categorias de tarefas de análise:

- **Tarefas do Sistema** - contém a lista das tarefas por defeito do sistema. As seguintes tarefas estão disponíveis:

  **Análise Completa**

  Analisa todo o sistema, excepto arquivos.Na configuração por defeito, analisa todos os tipos de malware excepto rootkits.

  **Análise Rápida**

  A Análise Rápida utiliza a análise nas nuvens para detectar malware em execução no seu sistema.Normalmente, a realização de uma Análise Rápida demora menos de um minuto e utiliza uma facção dos recursos do sistema necessários para uma análise de vírus normal.

  **Análise Autologon**

  Analisar os itens que são executados quando o utilizador entra no Windows.Por defeito, a análise ao logon está desactivada.

  Se deseja usar esta tarefa, faça clique botão direito nela, selecione **Agendar** e defina a tarefa para ser executada no**arranque do sistema**.Pode definir quanto tempo após o iniciar do sistema a tarefa deve de ser iniciada.

  **Análise Minuciosa**

  Analisa todo o sistema.Na configuração por defeito, faz uma nálise em busca de todo o tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.

  Nota

  Um vez que as atrefas **Análise Minuciosa do Sistema** e **Análise Completa do Sistema** analisam todo o sistema, a análise deverá demorar um pouco. Por isso, recomendamos que execute estas tarefas com baixa prioridade ou, melhor, quando o seu sistema estiver inactivo.

- **Tarefas do Utilizador** - contém as tarefas definidas pelo utilizador.

Uma tarefa chamada `Os Meus Documentos` é fornecida.Use esta tarefa para analisar pastas de utilizadores actuais: `Os Meus Documentos`, `Ambiente de Trabalho` e `StartUp`. Isto irá assegurar a segurança dos seus documentos, uma área de trabalho segura e aplicações limpas a serem executadas no arranque.

- **Tarefas Misc** - contém uma lista de tarefas de análise variadas. Estas tarefas de análise dizem respeito a tipos de análise alternativas que não podem ser executadas a partir desta janela. Apenas pode modificar as suas configurações ou ver os relatórios de análise.As seguintes tarefas estão disponíveis:

  **Análise de Dispositivos**

  O BitDefender pode detectar automaticamente sempre que é ligado um dispositivo de armazenamento ao computador e analisá-lo.Utilize esta tarefa para configurar as opções da detecção e análise automática de dispositivos de armazenamento (CDs/DVDs, dispositivos USB ou unidades de rede mapeadas).

  **Menu Contextual da Análise**

  Esta tarefa é utilizada na análise a partir do menu de contexto do Windows ou da barra de actividade de análise.Pode modificar as opções de análise consoante as suas necessidades.

Pode gerir as tarefas de análise com os botões ou com o menu de atalho.

Para levar a cabo uma tarefa de análise do sistema ou definida por si, clique no botão **Executar Tarefa** button.O Assistente de Análise Antivírus irá surgir e guiá-lo através do processo de análise.

Para definir a execução automática de uma tarefa de análise, mais tarde ou regularmente, clique no respectivo botão **Agendar** e configure o agendamento da tarefa consoante o necessário.

Se já não precise de uma tarefa de análise que criou, pode pagá-la clicando no botão **Apagar** localizado do lado direito da tarefa.Não pode apagar tarefas de sistema ou variadas.

Cada tarefa de análise possui uma janela de Propriedades, onde pode configurar as definições e ver os relatórios de análise.Para abrir esta janela clique em **Propriedades** localizado no botão do lado esquerdo da tarefa (ou clique com o botão direito do rato na tarefa e depois clique em **Propriedades**).

Para saber mais, consulte os seguintes tópicos:

- "*Configurar Definições da Análise*" (p. 71)
- "*Definir Alvo da Análise*" (p. 74)
- "*Agendar Tarefas de Análise*" (p. 74)

## Usando o Menú de Atalho

Um menú de atalho está disponível para cada tarefa. Clique com o botão direito do rato sobre a tarefa para a abrir.

Para as tarefas de sistema ou definidas pelo utilizador, os seguintes comandos estão disponíveis no menu de atalhos:

- **Analisar Agora** - executa a tarefa seleccionada, dando início a uma análise imediata.
- **Caminho** - Abre a janela das **Propriedades**, botão Caminho onde pode modificar o alvo da análise para a tarefa seleccionada.No caso de tarefas do sistema, esta opção é substituida por **Mostrar Caminhos de Análise**, onde apenas poderá ver o alvo da sua análise.
- **Agendar** - abre a janela das **Propriedades** e o botão Agendar, onde pode agendar a tarefa seleccionada.
- **Relatórios** - abre a janela das **Propriedades** e o botão Relatórios onde pode ver os relatórios gerados após as tarefas seleccionadas terem sido executadas.
- **Duplicar Tarefa** - duplica a tarefa seleccionada.Isto é útil na criação de novas tarefas, pois pode modificar as definições da tarefa duplicada.
- **Apagar** - elimina a tarefa seleccionada.

Nota

Disponível apenas para tarefas criadas pelo utilizador. Não pode remover uma tarefa predefinida.

- **Propriedades** - abra a janela **Propriedades**, e o botão Geral , onde pode modificar as configurações para a tarefa seleccionada.

Devido à sua natureza em particular, das **Tarefas Misc** categoria, apenas **Ver Relatório** e **Propriedades** estão disponíveis neste caso.

## Configurar Definições da Análise

Para configurar as opções de análise de uma específica tarefa de análise, faça clique-botão direito e seleccione **Propriedades**.

Pode facilmente configurar as opções de análise ajustando o nível de análise. Arraste o cursor ao longo da escala para definir o nível de análise pretendido.Utilize a descrição do lado direito da escala para escolher o nível de análise que melhor se adequa às suas necessidades.

Também pode configurar as seguintes opções gerais:

- **Execute a tarefa de análise com prioridade baixa.** Diminui a prioridade do processo de análise. Irá permitir que outros programas funcionem com maior rapidez e aumenta o tempo necessário para terminar o processo da análise.
- **Minimizar a janela da análise para a área de notificação.** Minimiza a janela da análise no Windows para a área de notificação. Faça duplo-clique sobre o ícone BitDefender para o abrir.
- Especifique a acção a aplicar se não forem encontradas ameaças.

Os utilizadores avançados poderão querer tirar partido das configurações de análise que o BitDefender oferece. O analisador pode ser configurado para evitar extensões de ficheiros, directorias ou arquivos que sabe serem inofensivos. Isto poderá reduzir o tempo de análise e melhorar a resposta do seu computador durante uma análise.

Para configurar em detalhe as definições de análise:

1. Clique em **Personalizar**.
2. Configure as definições de análise como necessário.Para saber o que uma opção faz, mantenha o rato sobre a mesma e leia a descripção apresentada no fundo da janela.
3. Clique em **OK** para guardar as alterações e fechar a janela.

Poderá achar esta informação útil:

- Se não está familiarizado com alguns dos termos, procure-os no glossário.Pode também encontrar informação útil pesquisando a Internet.
- **Nível de Análise.** Especifique que tipo de malware quer que o BitDefender analise seleccionando as opções apropriadas.
- **Análise de ficheiros.** Pode definir o BitDefender para analisar todos os ficheiros acedidos, apenas aplicações (ficheiros de programa) ou tipos de ficheiro específicos que achar perigosos.A análise de todos os ficheiros proporciona uma maior segurança, enquanto a análise das aplicações só pode ser utilizada numa análise mais rápida.

  As aplicações (ou ficheiros de programa) são muito mais vulneráveis a ataques de malware do que qualquer outro tipo de ficheiros.Esta categoria inclui as seguintes extensões de ficheiro:`.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml`; `.nws`.

  Se optar por **Analisar extensões definidas pelo utilizador**, é recomendado que inclua todas as extensões de aplicação para além das extensões de ficheiros que considere perigosas.

- **Analisar só ficheiros alterados.** Ao analisar apenas ficheiros novos e modificados, pode melhorar significativamente o desempenho do seu sistema sem comprometer a sua segurança.
- **Analisar dentro dos arquivos.** Os arquivos que contém ficheiros infectados não são uma ameaça imediata à segurança do seu sistema.O malware só pode afectar o seu sistema se o ficheiro infectado for extraído do arquivo e executado sem que a protecção em tempo real esteja activada.No entanto, é recomendado que utilize esta opção para detectar e remover qualquer ameaça potencial, mesmo se não for imediata.

Nota
Analisar ficheiros arquivados aumenta o tempo da análise e requer mais recursos do sistema.

- **Opções de acção.** Especifique as ações a serem tomadas em cada categoria de ficheiros detectados usando as opções nesta categoria.Há três categorias de ficheiros detectados:
  - **Ficheiros infectados.** Os ficheiros detectados como infectados correspondem a uma assinatura de malware na Base de Dados de Assinaturas de Malware do BitDefender.Por norma, o BitDefender consegue remover o código de malware de um ficheiro infectado e reconstruir o ficheiro original. Esta operação é conhecida por desinfecção.

Nota
As assinaturas de malware são fragmentos de código extraídos de amostras de malware. São utilizados por programas antivírus para efectuar correspondência entre padrões e detectar malware.
A Base de Dados de Assinatura de Malware BitDefender é uma colecção de assinaturas de malware actualizada a toda hora pelos investigadores de malware da BitDefender.

  - **Ficheiros suspeitos.** Os ficheiros são detectados como suspeitos pela análise heurística.Não foi possível desinfectar os ficheiros suspeitos por não estar disponível uma rotina de desinfecção.
  - **Ficheiros ocultos (rootkits).** Repare que este ficheiros ocultos, não são os ficheiros que esconde deliberadamente no Windows. Eles são ficheiros ocultos por programas especiais, conhecidos como rootkits.Os rootkits não são maliciosos por natureza, No entanto, eles são vulgarmente utilizados para tornar os vírus ou o spyware indetectáveis pelos programas antivírus.

  Não deve alterar a acções predefinidas aplicadas aos ficheiros detectados excepto se tiver uma forte razão para isso.

Para definir uma nova acção, clique na actual **Primeira acção** e seleccione a opção desejada a partir do menu.Especifique uma **Acção secundária** caso haja falha na principal.

Clique em **OK** para guardar as alterações e fechar a janela. Para executar a tarefa, apenas clique em **Analisar**.

## Definir Alvo da Análise

Não pode modificar os alvos de análise das tarefas de análise a partir da categoria **tarefas do Sistema**.Apenas pode ver o alvo da análise deles.Para ver o alvo da análise de uma determinada tarefa de análise do sistema, faça clique com o botão direito do rato sobre a tarefa e seleccione **Mostrar Caminho da Análise**.

Para definir o alvo da análise de uma determinada tarefa de análise, clique botão direito na tarefa e seleccione **Caminhos**. Alternativamente, se já se encontra na janela das Propriedades da tarefa, seleccione a barra **Caminhos**.

Pode ver a lista das drives locais amovíveis e de rede, como também, se houver, os ficheiros e as pastas adicionada previamente. Todos os items seleccionados serão analisados quando a tarefa for executada.

Estão disponíveis os seguintes botões:

- **Adicionar Itens** - abre uma janela de exploração, onde pode seleccionar o(s) ficheiro(s) e pasta(s), que pretende analisar.

Nota
Use carregar & descarregar para adicionar à lista ficheiros/pastas.

- **Apagar item** - remove o(s) ficheiro (s) / pasta(s) que foram previamente seleccionados da lista dos objectos a serem analisados.

Para além destes botões, existem algumas opções que permitem uma selecção rápida das áreas a analisar.

- **Unidades Locais** - para analisar as drives locais.
- **Unidades de Rede** - para analisar todas as drives de rede.
- **Unidades Amovíveis** - para analisar todas as drives amovíveis (CD-ROM, unidade de disquetes).
- **Todas as Entradas** - para analisar todos as drives, independentemente de serem locais, de rede ou amovíveis.

Clique em **OK** para guardar as alterações e fechar a janela. Para executar a tarefa, apenas clique em **Analisar**.

## Agendar Tarefas de Análise

Com tarefas complexas, o processo de análise leva algum tempo, e funciona melhor se fechar todos os outros programas. É por isso que é melhor agendar tais tarefas

para quando não estiver a utilizar o seu computador e este tenha entrado no modo de descanso.

Para ver o agendamento de uma determinada tarefa ou modificá-lo, clique botão direito do rato e seleccione **Agendar**. Se já se encontra na janela das Propriedades, seleccione a barra **Agendador**.

Se houver, pode ver a tarefa agendada.

Quando agendar uma tarefa, deve de escolher uma das seguintes opções:

- **Não** - executa a tarefa apenas quando o utilizador a solicita.
- **Uma vez** - Executa a análise uma só vez, num determinado momento. Definir a data de início e a hora nos campos**Iniciar Data/Hora**
- **Periodicamente** - Executa a análise periodicamente, num determinado intervalo de tempo (horas, dias, semanas, meses, anos) começando a uma determinada data e hora.
- **No iniciar do sistema** - Executa a análise, após um determinado número de minutos especificados, após o utilizador entrar no Windows.

Clique em **OK** para guardar as alterações e fechar a janela. Para executar a tarefa, apenas clique em **Analisar**.

## 15.3. Configurar Exclusões da Análise

Há casos em que tem de excluir certos ficheiros de serem analisados. Por exemplo, poderá querer excluir um ficheiro de teste EICAR da análise no acesso ou os ficheiros `.avi` da análise a pedido.

BitDefender permite-lhe excluir objectos da análise no-acesso e da análise a-pedido, ou de ambas. Esta definição tem o propósito de diminuir o tempo de análise e evitar interferência com o seu trabalho.

Dois tipos de objectos podem ser excluidos da análise:

- **Caminhos** - o ficheiro ou pasta (incluindo os objectos que contém) indicados por um determinado caminho serão excluídos da análise.
- **Extensões** - todos os ficheiros com a extensão especificada serão excluídos da análise, independentemente da localização no disco rígido.

Os objectos excluídos da análise a-pedido não serão analisados, independentemente de eles serem acedidos por si ou por uma aplicação.

Nota

As exclusões NÃO serão aplicadas à análise contextual.Análise Contextual é um tipo de análise a-pedido: você clica com o botão direito de rato sobre o ficheiro ou pasta que quer analisar e selecciona **Analisar com BitDefender**.

### 15.3.1. Excluir Ficheiros ou Pastas da Análise

Para excluir caminhos da análise:

1. Abrir o BitDefender.
2. Dependendo do modo de interface do utilizador, proceda da seguinte forma:

   Modo Intermédio

   Abra o separador **Segurança** e clique em **Configurar o Antivírus**, nas Tarefas Rápidas, no lado esquerdo da janela.

   Vá ao separador **Exclusões**.

   Modo Avançado

   Vá a **Antivírus > Exclusões**.

   Nota

   No Modo Básico e no Modo Intermédio, pode configurar um atalho para poder aceder a estas definições a partir do painel de instrumentos.Para mais informação, por favor consulte o "*Ferramentas*" (p. 30).

3. Seleccione a respectiva caixa para activar as exclusões de análise.
4. Inicie o assistente de configuração da seguinte forma:
   - Clique com o botão direito na tabela Ficheiros e Pastas e seleccione **Adicionar novo caminho**.
   - Clique no botão **Adicionar**, localizado no cimo da tabela de exclusões.
5. Siga o assistente de configuração.Pode navegar pelo assistente utilizando os botões **Seguinte** e **Retroceder**.Para sair do assistente, clique em **Cancelar**.
   a. Seleccione a opção de excluir um caminho da análise.Este passo só aparece quando inicia o assistente clicando no botão **Adicionar**.
   b. Para especificar os caminhos a excluir da análise use os seguintes métodos:
      - Clique em **Explorar**, seleccione o ficheiro ou pasta que deseja excluir da análise e depois clique **Adicionar**.
      - Insira o caminho que deseja que seja excluído da análise no campo editado e clique em **Adicionar**.

      Os caminhos surgirão na lista à medida que os adicione. Pode adicionar tantos caminhos quanto os que deseje.
   c. Por defeito, os caminhos seleccionados são excluídos da análise no-acesso e a-pedido. Para alterar isto, clique na coluna à direita e seleccione a opção desejada da lista.

d. É altamente recomendável analisar os ficheiros nos caminhos especificados para ter a certeza de que não estão infectados.Seleccione a caixa de selecção para analisar estes ficheiros antes de os excluir da análise.

Clique em **Concluir** para adicionar exclusões da análise.

6. Prima **Aplicar** para guardar as alterações.

### 15.3.2. Excluir Extensões de Ficheiros da Análise

Para excluir extensões de ficheiro da análise:

1. Abrir o BitDefender.
2. Dependendo do modo de interface do utilizador, proceda da seguinte forma:

Modo Intermédio

Abra o separador **Segurança** e clique em **Configurar o Antivírus**, nas Tarefas Rápidas, no lado esquerdo da janela.

Vá ao separador **Exclusões**.

Modo Avançado

Vá a **Antivírus > Exclusões**.

Nota

No Modo Básico e no Modo Intermédio, pode configurar um atalho para poder aceder a estas definições a partir do painel de instrumentos.Para mais informação, por favor consulte o "*Ferramentas*" (p. 30).

3. Seleccione a respectiva caixa para activar as exclusões de análise.
4. Inicie o assistente de configuração da seguinte forma:
   - Clique com o botão direito na tabela de Extensões e seleccione **Adicionar novas extensões**.
   - Clique no botão **Adicionar**, localizado no cimo da tabela de exclusões.
5. Siga o assistente de configuração.Pode navegar pelo assistente utilizando os botões **Seguinte** e **Retroceder**.Para sair do assistente, clique em **Cancelar**.
   a. Seleccione a opção de excluir extensões da analiseEste passo só aparece quando inicia o assistente clicando no botão **Adicionar**.
   b. Para especificar as extensões a serem excluídas da análise use os seguintes métodos:
      - Seleccione a partir do menu a extensão que deseja excluir da análise e clique em **Adicionar**.

Nota
O menu contém uma lista de extensões registadas no seu sistema. Quando selecciona uma extensão, pode ver a sua descripção, caso a mesma esteja disponível.

- Insira a extensões que deseja excluir da análise no campo editar e clique em **Adicionar**.

As extensões aparecerão na lista à medida que as adiciona. Pode adicionar tantas extensões quantas as que desejar.

c. Por defeito, as extensões seleccionadas são excluidas da análise no-acesso e a-pedido. Para alterar isto, clique na coluna da direita e seleccione a opção que deseja a partir da lista.

d. É altamente recomendável analisar os ficheiros com as extensões especificadas para ter a certeza de que não estão infectados.

Clique em **Concluir** para adicionar exclusões da análise.

6. Prima **Aplicar** para guardar as alterações.

### 15.3.3. Gerir Exclusões da Análise

Se as exclusões de análise configuradas já não forem necessárias, é recomendado que elimine ou desactive as exclusões da análise.

Para gerir as exclusões da análise:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Antivírus > Exclusões**.

Para eliminar um item da lista, seleccione-o e clique no botão **Apagar**.

Para editar uma entrada da lista, seleccione-a e clique no botão **Editar**.Aparecerá uma nova janela onde poderá alterar a extensão ou o caminho a ser excluído e o tipo de análise da qual quer que eles sejam excluídos. Faça as alterção necessárias e clique **OK**.

Nota
Pode também clicar no objecto usando o botão direito do rato e utilizar as opções que aparecem no menu de atalho para o editar ou apagar.

Para desactivar exclusões de análise, desmarque a respectiva caixa de selecção.

## 15.4. Àrea de Quarentena

O BitDefender permite o isolamento de ficheiros infectados ou suspeitos numa área segura, chamada de quarentena. Ao isolar estes ficheiros na quarentena, desaparece

o risco de infecção,e ao mesmo tempo, terá a possibilidade de enviar estes ficheiros para análise no laboratório do BitDefender.

Nota

Quando o vírus se encontra na quarentena não pode provocar nenhum mal, porque não pode ser nem lido nem executado.

Em adição, o BitDefender analisa os ficheiros em quarentena após cada actualização das assinaturas de malware.Os ficheiros limpos são automaticamente repostos no seu local de origem.

Para ver e gerir os ficheiros na quarentena e configurar as definições da quarentena:

1. Abrir o BitDefender.
2. Dependendo do modo de interface do utilizador, proceda da seguinte forma:

   Modo Intermédio

   Abra o separador **Segurança** e clique em **Configurar o Antivírus**, nas Tarefas Rápidas, no lado esquerdo da janela.

   Abra o separador **Quarentena**.

   Modo Avançado

   Vá a **Antivírus > Quarentena**.

Nota

No Modo Básico e no Modo Intermédio, pode configurar um atalho para poder aceder a estas definições a partir do painel de instrumentos.Para mais informação, por favor consulte o "*Ferramentas*" (p. 30).

## Gerir Ficheiros em Quarentena

Pode enviar qualquer ficheiro seleccionado da quarentena para os Laboratórios BitDefender clicando no botão **Enviar**.Por defeito o BitDefender envia automaticamente os ficheiros em quarentena a cada 60 minutos.

Para eliminar um ficheiro da quarentena, seleccione-o e clique no botão **Eliminar**.

Se pretende restaurar um ficheiro da quarentena para a respectiva localização original, seleccione-o e clique em **Restaurar**.

## Configuração da Quarantena

Para configurar as definições da quarentena, clique em **Configuração**.Ao usar a configuração da quarentena, pode definir o BitDefender para executar automaticamente as seguintes acções:

**Apagar ficheiros antigos.** Para apagar automaticamente ficheiros antigos da quarentena, seleccione a opção correspondente.Deve especificar o número de dias

após os quais os ficheiros em quarentena deverão ser apagados e a frequência com a qual o BitDefender deve de verificar esta situação.

**Enviar os ficheiros automaticamente.** Para enviar automaticamente ficheiros em quarentena, seleccione a opção correspondente.Deve de especificar a frequência com que deseja enviar os ficheiros.

**Analisar os ficheiros em quarentena após a actualização.** Para analisar automaticamente ficheiros em quarentena após a actualização, seleccione a opção correspondente.Pode escolher mover automaticamente os ficheiros limpos para a sua localização original seleccionado a opção **Restaurar Ficheiros Limpos**.

Clique em **OK** para guardar as alterações e fechar a janela.

# 16. Protecção Antiphishing

O BitDefender Antiphishing impede que seja revelada informação pessoal enquanto explora a internet ao alertá-lo acerca das páginas web potencialmente phishing.

O BitDefender dá-lhe uma protecção Antiphishing em tempo-real para:

- Internet Explorer
- Mozilla Firefox
- Yahoo! Messenger
- Windows Live (MSN) Messenger

## 16.1. Configurar a Lista Branca de Antiphishing

Pode configurar e gerir uma lista branca de sítios de Internet que não serão analisados pelos motores Antiphishing do BitDefender.A lista branca deve de conter apenas os websites em que confia plenamente.Por exemplo, adicione os websites onde costuma frequentemente fazer compras on-line.

Nota

Pode de forma fácil e eficiente gerir a protecção antiphishing e a Lista Branca usando a barra de ferramentas do BitDefender Antiphishing que está integrada no Internet Explorer.Para mais informação, por favor consulte o *"Gerir a Protecção Antiphishing do BitDefender no Internet Explorer e Firefox"* (p. 81).

Para configurar e gerir a lista branca de antiphishing:

- Se estiver a usar um navegador da Internet compatível, clique na barra de ferramentas do BitDefender e seleccione **Lista Branca** no menu.
- Em alternativa, proceda da seguinte forma:
  1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
  2. Vá a **Antivírus > Escudo**.
  3. Clique em **Lista Branca**.

Para adicionar um site à Lista Branca, insira o seu endereço no campo correspondente e depois clique em **Adicionar**.

Para remover um site web da lista branca, seleccione-a e clique **Remover**.

Clique em **Guardar** para guardar as alterações e fechar a janela.

## 16.2. Gerir a Protecção Antiphishing do BitDefender no Internet Explorer e Firefox

BitDefender integra-se directamente através de uma barra de tarefas intuitiva e fácil de usar nos seguintes exploradores da Internet:

- Internet Explorer
- Mozilla Firefox

Pode de forma fácil e eficiente gerir a protecção antiphishing e a Lista Branca usando a barra de ferramentas do BitDefender Antiphishing que está integrada num dos exploradores da internet acima.

A barra de ferramentas antiphishing representado pelo ícone do BitDefender, encontra-se no lado superior do Explorador da Internet.Clique nele de forma a abrir o menu da barra de ferramentas.

Nota

Se não consegue ver a barra de ferramentas, abra o menu **Ver** siga para **Barras de ferramentas** e seleccione **Barra de Ferramentas BitDefender**.

Os seguintes comandos estão disponíveis no menu da barra de ferramentas:

- **Activar / Desactivar** - activa / desactiva a barra de ferramentas Antiphishing do BitDefender, no presente explorador de internet.
- **Configuração** - abre uma janela onde pode especificar as definições da barra de ferramentas do antiphishing.Estão disponíveis as seguintes opções:
  - **Protecção Antiphishing Wen em Tempo-real** - detecta e alerta-o em tempo-real se um site web é de phishing (preparado para lhe roubar informação pessoal).Esta opção controla a protecção antiphishing BitDefender apenas no actual explorador da internet.
  - **Avisar antes adicionar à lista branca** - será consultado antes de ser adicionado um site web à Lista Branca.
- **Adicionar à Lista Branca** - adiciona o actual site web à Lista Branca.

Importante

Adicionar um site à Lista Branca significa que o BitDefender não irá mais analisar esse site em busca de tentativas de phishing. Recomendamos que adicione à Lista Branca apenas os sites em que confia totalmente.

- **Lista Branca** - abre a Lista Branca.Para mais informação, por favor consulte o "*Configurar a Lista Branca de Antiphishing*" (p. 81).
- **Relatar como Phishing** - informa o Laboratório BitDefender que você considera determinado site web como sendo usado para phishing.Ao reportat sites de phishing você ajuda a proteger outros contra o roubo de identidade.
- **Ajuda** - abre a documentação electrónica.
- **Acerca** - abre uma janela onde pode ver informação acerca do BitDefender e onde procurar ajuda caso algo de inesperado lhe apareça.

# 17. Consultor de Procura

O Consultor de Procura melhora a protecção contra ameaças em linha alertando sobre páginas da Internet de phishing ou inseguras directamente na página com os resultados das suas pesquisas.

O Consultor de Procura é compatível com todos os navegadores de Internet e analisa os resultados da pesquisa apresentados pelos motores de busca mais conhecidos:

- Google
- Yahoo!
- Bing

O Consultor de Procura indica se um resultado da pesquisa é seguro ou não, colocando um pequeno ícone de estado antes da hiperligação.

**Círculo verde com uma marca de verificação:** Pode aceder com segurança à hiperligação.

**Circulo vermelho com um ponto de exclamação:** Esta é uma página de Internet de phishing ou que não é de confiança.Deve evitar abrir esta hiperligação.Se estiver a utilizar o Internet Explorer ou o Firefox e tentar abrir a hiperligação, o BitDefender irá bloquear automaticamente a página de Internet e apresentar antes uma página de alerta.Se pretende ignorar o alerta e aceder à página de Internet, siga as instruções na página de alerta.

## 17.1. Desactivar o Consultor de Procura:

Para desactivar o Consultor de Procura:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Preferências**.
2. Vá a **Definições de Segurança**.
3. Utilize o botão para desactivar o Consultor de Procura.

# 18. Controlo de Privacidade

BitDefender monitoriza dezenas de potenciais "hotspots" no seu sistema onde o spyware poderá actuar, e também verifica quaisquer mudanças feitas ao seu sistema e ao seu software. É bastante eficaz no bloqueio de cavalos de Tróia e outras ferramentas instaladas por hackers, que tentam comprometer a sua privacidade e enviar a sua informação pessoal, tal como números de cartão de crédito, do seu computador para o do hacker.

O Controlo de Privacidade inclui os seguintes componentes:

- Controlo de Identidade - ajuda a garantir que os seus dados pessoais não são enviados a partir do computador sem o seu consentimento. Analisa as mensagens electrónicas e instantâneas enviadas do computador, assim como todos os dados enviados através de páginas da Internet, e bloqueia toda a informação protegida pelas regras de Controlo de Identidade que criou.
- O Controlo do Registo - irá pedir a sua permissão sempre que um programa tentar modificar uma entrada de registo de forma a poder ser executado durante o arranque do Windows.
- O Controlo de Cookies - irá pedir a sua permissão sempre que um novo site web tentar definir uma cookie.
- O Controlo de script - irá pedir a sua permissão sempre que um site web tente activar um script ou outro conteúdo activo.

Por defeito, apenas o Controlo de Identidade está activado.Tem de configurar correctamente as regras do Controlo de Identidade para impedir o envio não autorizado de informações confidenciais.Para mais informação, por favor consulte o "*Configurar o Controlo de Identidade*" (p. 86).

Os outros componentes do Controlo de Privacidade são interactivos. Se os activar, ser-lhe-á pedido, em janelas de alerta, que autorize ou bloqueie certas acções quando estiver a navegar na Internet ou a instalar novo software. É por isso que é, normalmente, utilizado por utilizadores mais experientes.

## 18.1. Configurar Nível de Protecção

O nível de protecção ajuda-o a activar ou desactivar facilmente os componentes do Controlo de Privacidade.

Para configurar o nível de protecção:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Controlo de Privacidade > Estado**.
3. Certifique-se que o Controlo de Privacidade está activado.

4. Há duas opções:

   - Arraste o cursor pela escala para definir o nível de protecção apropriada.Clique em **Nível por Defeito** para colocar o mostrador no nível por defeito.

     Utilize a descrição do lado direito da escala para escolher o nível de protecção que melhor se adequa às suas necessidades de segurança.

   - Pode personalizar o nível de protecção clicando em **Nível Pessoal**.Na janela que lhe irá aparecer, escolha o controlos de protecção que deseja activar e clique em **OK**.

## 18.2. Controlo de identidade

O Controlo de Identidade protege-o contra o roubo de informação sensível quando se encontra on-line.

Imagine a seguinte situação: criou uma regra de Controlo de Identidade para proteger o número do seu cartão de crédito.Se, de alguma forma, um software espião conseguir instalar-se no seu computador, não conseguirá enviar o número do seu cartão de crédito em mensagens de correio electrónico, mensagens instantâneas ou páginas de Internet. Além disso, os seus filhos não poderão utilizá-lo para fazer compras em linha ou revelá-lo a pessoas que conheceram na Internet.

Para saber mais, consulte os seguintes tópicos:

- "*Sobre o Controlo de Identidade*" (p. 85).
- "*Configurar o Controlo de Identidade*" (p. 86).
- "*Gerir Regras*" (p. 89).

### 18.2.1. Sobre o Controlo de Identidade

Manter informação confidencial segura é um assunto importante que nos preocupa a todos. O roubo de dados tem crescido com o desenvolvimento das comunicações Internet e actualmente fazem-se uso de novos métodos para enganar as pessoas e retirar-lhes informação privada.

Quer seja o seu e-mail o seu número de cartão de crédito, quandos eles caem em mãos erradas essa informação poderá causar-lhe danos: poderá encontrar-se afogado em mensagens spam ou poderá ser surpreendido ao aceder à sua conta e verificar que está vazia.

O Controlo de Identidade protege-o contra o roubo de informação sensível quando se encontra on-line.Baseado nas regras que criar, o Controlo de Identidade analisa o tráfego web, de e-mail e de mensagens instantâneas que sai do seu computador em busca de chaves de caracteres específicos (por exemplo, o seu número de cartão de crédito). Se houver uma correspondência, a respectiva página web, e-mail ou mensagem instantânea é bloqueada.

Pode criar regras para proteger cada peça de informação que possa considerar pessoal ou confidencial, desde o seu número de telefone ou endereço de e-mail até à sua informação bancária.Suporte multi-utilizador é fornecido de forma a que os utilizadores de diferentes contas do Windows possam configurar e usar as suas próprias regras de identidade.Se a sua conta de Windows é uma conta de administrador, as regras que cria podem ser configuradas para também se aplicarem a utilizadores de outras contas do computador.

Porquê usar o Controlo de Identidade?

- O Controlo de Identidade é bastante eficaz a bloquear spyware keylogger.Este tipo de aplicações maliciosas grava as teclas que pressionou no teclado e envia-as para a Internet para uma pessoa maliciosa (hacker).O hacker pode descobrir informação sensível a partir de dados roubados, tais como números de contas bancárias e palavras-passe, e usá-las em benefício pessoal.

  Supondo que tal aplicação funciona de forma a evitar a detecção antivírus, a mesma não pode enviar os dados roubados por e-mail, web ou mensagens instântaneas se tiver criado as regras de protecção de identidade adequadas.

- O Controlo de Identidade protege-o contra as tentativas de phishing (tentativas de roubar informação pessoal).As tentativas de phishing mais comuns fazem uso de um e-mail enganador para o levar a inserir informação pessoal numa página web falsa.

  Por exemplo, poderá receber um e-mail a fingir que é do seu banco a pedir-lhe que actualize os dados da sua conta bancária com urgência.O e-mail traz um link para uma página web onde deve de inserir a sua informação pessoal.Apesar de parecerem legítimos, o e-mail e o link para a página web são falsos.Se clicar no link do e-mail e inserir a sua informação pessoal na página web falsa, estará a revelar esta informação às pessoas maliciosas que organizaram a tentativa de phishing.

  Se as regras de protecção de identidade estiverem feitas, não poderá enviar informação pessoal (tal como o número do seu cartão de crédito) para uma página web a não ser que tenha definido essa página web como uma excepção.

- Com as regras do Controlo de Identidade, pode evitar que os seus filhos forneçam informações pessoais (por exemplo, a morada ou o número de telefone) a pessoas que conheceram na Internet. Além disso, se criar regras para proteger o seu cartão de crédito, eles não poderão fazer compras sem o seu consentimento.

### 18.2.2. Configurar o Controlo de Identidade

Se deseja usar p Controlo de Identidade, siga estes passos:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Controlo de Privacidade > Identidade**.

3. Certifique-se que o Controlo de Identidade está activado.

Nota
Se não for possível configurar a opção, vá ao separador **Estado** e active o Controlo de Privacidade.

4. Criar regras para proteger a sua informação sensível.Para mais informação, por favor consulte o "*Criar Regras de Controlo de Identidade*" (p. 87).
5. Se necessário, defina excepções específicas para as regras que criou.Por exemplo, se criou uma regra para proteger o número do seu cartão de crédito, adicione os sítios de Internet onde normalmente utiliza o cartão de crédito à lista de exclusões.Para mais informação, por favor consulte o "*Definir Excepções*" (p. 88).

## Criar Regras de Controlo de Identidade

Para criar uma regra de protecção de identidade clique no botão **Adicionar** e siga o assistente de configuração.Pode navegar pelo assistente utilizando os botões **Seguinte** e **Retroceder**.Para sair do assistente, clique em **Cancelar**.

1. **Janela de boas-vindas**
2. **Definir Tipo de Regra e Dados**

   Deve definir os seguintes parâmetros:

   - **Nome Regra** - insira o nome da regra no campo editável.
   - **Tipo de Regra** - escolha o tipo de regra (morada, nome, cartão de crédito, PIN, NSS, etc.
   - **Dados Regra** - insira os dados que quer proteger com a regra no campo editável.Por exemplo, se deseja proteger o seu número de cartão de crédito, insira o mesmo ou parte dele aqui.

Importante
Se inserir menos do que três caracteres, será notificado a validar os dados. Recomendamos que insira pelo menos três caracteres de forma a evitar o bloqueio por engano de mensagens e páginas web.

   Todos os dados que inserir são encriptados. Para uma segurança adicional, não insira a totalidade dos dados que deseja proteger.

3. **Seleccione Utilizadores e Tipo de Trafego.**

   a. Seleccione o tráfego que quer que o BitDefender analise.

   - **Analisar Web (tráfego HTTP)** - analisa o tráfego HTTP (web) e bloqueia os dados de saída que correspondem aos dados da regra.

- **Analisar e-mail (tráfego SMTP)** - analisa todo o tráfego SMTP (mail) e bloqueia as mensagens de e-mail de saída que contém os dados da regra.
- **Analisar Mensagens Instantâneas** - analisa todo o tráfego Mensagens Instantâneas e bloqueia as mensagens de chat de saída que contenham os dados da regra.

Pode escolher aplicar a regra apenas se a mesma corresponder em todas as palavras ou se os dados da regra e os caracteres detectados correspondem em termos de letra (Maiúsculas, minúsculas).

b. Específique para que utilizadores se aplicam as regras.

- **Apenas para mim (utilizador actual)** - a regra será aplicada à sua conta de utilizador.
- **Utilizadores limitados** - a regra será aplicada a si e a todas as contas de Windows limitadas.
- **Todos os utilizadores** - a regra será aplicada a todas contas do Windows.

4. **Descrever Regra**

Insira uma breve descrição da regra no campo de edição.Um vez que os dados bloqueados (string de caracteres) não são mostrados em pleno texto quando se acede à regra, a descripção deverá ajudá-lo a identificá-la facilmente.

Clique em **Terminar**.A regra aparecerá na tabela.

A partir se agora, qualquer tentativa para enviar os dados especificados (por correio electrónico, mensagens electrónicas ou páginas da Internet) irá falhar. Será apresentada uma mensagem de alerta indicando que o BitDefender impediu o envio de elementos de identificação.

## Definir Excepções

Há casos em que necessita de definir excepções para especificar as regras de identidade.Consideremos o caso em que criou uma regra que evita que o número do seu cartão de crédito seja enviado por HTTP (web). Sempre que o seu cartão de crédito seja submetido num site web a partir da sua conta de utilizador, a respectiva página web é bloqueada. Se deseja por exemplo, pagar uma compra online numa loja virtual (que você sabe ser segura), terá de especificar uma excepção para a respectiva regra.

Para abrir a janela onde pode gerir as excepções, clique em **Excepções**.

Para adicionar uma excepção, siga os seguintes passos:

1. Clique no botão **Adicionar** para adicionar a nova entrada à tabela.
2. Duplo-clique em **Especificar item excluído** e inserir o endereço web, endereço de e-mail ou o contacto IM que deseja adicionar como excepção.

3. Duplo-clique em**Tipo de Tráfego** e escolha do menu a opção correspondente ao tipo de endereço que inseriu anteriormente.
   - Se especificou um endereço web, seleccione **HTTP**.
   - Se especificou um endereço de e-mail, seleccione **Email (SMTP)**.
   - Se especificou um contacto IM, seleccione**IM**.

Para remover uma excepção da lista, seleccione-a e clique em **Remover**.

Clique em **Aplicar** para guardar as alterações.

### 18.2.3. Gerir Regras

Para gerir as regras do Controlo de Identidade:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Controlo de Privacidade > Identidade**.

Pode ver as regras criadas até agora listadas na tabela.

Para apagar uma regra, apenas seleccione-a e clique no botão **Apagar**.

Para editar uma regra, seleccione-a e clique no botão **Editar** ou faça duplo-clique sobre ela. Uma nova janela irá aparecer.Aqui pode mudar o nome, descripção e parâmetros da regra (tipo, dados e tráfego). Clique em **OK** para guardar as alterações.

## 18.3. Controlo de registo

Uma parte muito importante do sistema operativo do Windows é chamada de **Registo**. Aqui é o local onde o guarda as suas definições, programas instalados, informação acerca do utilizador e por aí a diante.

O **Registo** também é utilizado para definir quais os programas que deverão ser lançados automaticamente ao iniciar o Windows. Frequentemente, os vírus usam isto para se lançarem automaticamente quando o utilizador reiniciar o seu computador.

O **Controlo de registo** vigia o Registo do Windows – mais uma vez, isto é útil para detectar Cavalos de Tróia. Irá alertá-lo sempre que um programa tente modificar uma entrada de registo para poder ser executado ao iniciar o Windows.Para mais informação, por favor consulte o “*Alertas de Registo*” (p. 36).

Para configurar o Controlo de Registo:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Controlo de Privacidade > Registo**.
3. Seleccione a caixa respectiva para activar o Controlo de Registo.

Nota
Se não for possível configurar a opção, vá ao separador **Estado** e active o Controlo de Privacidade.

### Gerir Regras

Para apagar uma regra, apenas seleccione-a e clique no botão **Apagar**.

## 18.4. Controlo de cookies

As Cookies são uma ocurrência muito comum na Internet. Elas são ficheiros peqenos armazenados no seu computador. Os sites da Web criam estas cookies para manter o rasto da informação específica acerca de si.

As Cookies são geralmente criadas para facilitar a sua vida. Por exemplo, elas podem ajudar o site da Web a lembrar-se do seu nome e preferências, para que não tenha de as voltar a introduzir sempre que os visitar.

Mas as cookies também podem ser usadas para comprometer a sua privacidade, ao seguir o rasto das patentes da sua navegação.

É aqui que o Controlo de Cookies ajuda.Quando activado, o Controlo de Cookies vai pedir-lhe autorização sempre que um novo sítio de Internet tenta definir ou pedir um cookie.Para mais informação, por favor consulte o "*Alertas de Cookie*" (p. 37).

Para configurar o Controlo de Cookies:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Controlo de Privacidade > Cookie**.
3. Seleccione a caixa respectiva para activar o Controlo de Cookies.

   Nota
   Se não for possível configurar a opção, vá ao separador **Estado** e active o Controlo de Privacidade.

4. Pode configurar as regras para os sítios de Internet que visita regularmente, mas isto não é obrigatório.As regras são automaticamente criadas na janela de alertas, com base na sua resposta.

Nota
Devido ao grande número de cookies usadas hoje na Internet, o **Controlo de Cookie** pode ser um pouco aborrecido ao começo. Inicialmente, irá perguntar uma série de questões acerca de sites que tentam colocar cookies no seu computador. Logo que adicione os seus sites habituais à lista-regra, a navegação tornar-se-á tanto facilitada como anteriormente.

### Criar Regras Manualmente

Para adicionar manualmente uma regra, clique no botão **Adicionar** e configure os parâmetros da regra na janela de configuração.Pode definir os parâmetros:

- **Endereço de domínio** - introduza o domínio, no qual a regra deve aplicar-se.
- **Acção** - selecciona a acção da regra.

| Acção | Descrição |
|---|---|
| **Permitir** | Os cookies desse domínio serão executados. |
| **Bloquear** | Os cookies desse domínio não serão executados. |

- **Sentido** - selecciona o sentido do tráfego.

| Tipo | Descrição |
|---|---|
| **Saída** | A regra será aplicada apenas às cookies que são enviadas para fora do site conectado. |
| **Entrada** | A regra será aplicada apenas às cookies que são recebidas do site conectado. |
| **Ambos** | A regra aplica-se em ambos os sentidos. |

Nota

Pode aceitar cookies mas nunca as poderá devolver, ao estabelecer a acção para **Negar** e a direcção para **Saída**.

Clique em **Terminar**.

### Gerir Regras

Para apagar uma regra, apenas seleccione-a e clique no botão **Apagar**.Para alterar os parametros de uma regra, seleccione a regra no botão **Editar** ou faça duplo clique. Faça as alterações desejadas na janela de configuração.

## 18.5. Controlo de script

Escritas e outros códigos tais como Controlos de ActiveX e Java applets, os quais são usados para criar páginas da web interactivas, podem ser programados para ter efeitos inofensivos. Os elementos do ActiveX, por exemplo, podem ganhar total acesso aos seus dados e podem ler dados do seu computador, informação eliminada, capturar palavras-passe e interceptar mensagens enquanto você está em linha. Apenas deverá aceitar conteúdo activo de sites que conhece e confia totalmente.

Se activar o Controlo de Scripts, ser-lhe-á pedida autorização sempre que um novo sítio de Internet tentar executar um script ou outro conteúdo activo.Para mais informação, por favor consulte o "*Alertas de Script*" (p. 37).

Para configurar o Controlo de Script:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Controlo de Privacidade > Script**.
3. Seleccione a caixa respectiva para activar o Controlo de Script.

Nota
Se não for possível configurar a opção, vá ao separador **Estado** e active o Controlo de Privacidade.

4. Pode configurar as regras para os sítios de Internet que visita regularmente, mas isto não é obrigatório.As regras são automaticamente criadas na janela de alertas, com base na sua resposta.

## Criar Regras Manualmente

Para adicionar manualmente uma regra, clique no botão **Adicionar** e configure os parâmetros da regra na janela de configuração.Pode definir os parâmetros:

- **Endereço de domínio** - introduza o domínio, no qual a regra deve aplicar-se.
- **Acção** - selecciona a acção da regra.

| Acção | Descrição |
|---|---|
| **Permitir** | Os scripts desse domínio serão executados. |
| **Bloquear** | Os scripts desse domínio não serão executados. |

Clique em **Terminar**.

## Gerir Regras

Para apagar uma regra, apenas seleccione-a e clique no botão **Apagar**.Para alterar os parametros de uma regra, seleccione a regra no botão **Editar** ou faça duplo clique. Faça as alterações desejadas na janela de configuração.

# 19. Vulnerabilidade

Um passo importante na protecção do seu computador contra as pessoas e aplicações maliciosas é manter actualizado o seu sistema operativo e as aplicações que usa regularmente.Mais ainda, para evitar acesso físico não-autorizado ao seu computador, palavras-passe fortes (palavras-passe que não são fáceis de adivinhar) devem de ser criadas para cada conta de utilizador do Windows.

O BitDefender analisa regularmente o seu sistema em busca de vulnerabilidades e notifica-o das incidências existentes.

## 19.1. A analisar em busca de Vulnerabilidades

Pode verificar as vulnerabilidades e corrigi-las, passo a passo, com o assistente da **Análise de Vulnerabilidade**.Para iniciar o assistente, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Intermédio
: Abra o separador **Segurança** e clique em **Análise de Vulnerabilidade**, nas Tarefas Rápidas, no lado esquerdo da janela.

Modo Avançado
: Vá a **Vulnerabilidade > Estado** e clique em **Verificar Agora**.

Siga o procedimento de seis passos para remover as vulnerabilidades do seu sistema.Pode navegar pelo assistente utilizando o botão **Seguinte**. Para sair do assistente, clique em **Cancelar**.

1. **Proteja o seu PC**

   Seleccione as vulnerabilidades a verificar.

2. **Analisar incidências seleccionadas...**

   Aguarde que o BitDefender termine a análise de vulnerabilidades ao sistema.

3. **Actualizações do Windows**

   Pode ver a lista das actualizações criticas e não-criticas do Windows que não se encontram actualmente instaladas no seu computador.Seleccione as actualizações que pretende instalar.

4. **Actualizações das Aplicações**

   Se a aplicação não estiver actualizada, clique no link fornecido para descarregar a versão mais recente.

5. **Palavras-passe Fracas**

   Pode ver a lista dos utilizadores de contas Windows configurados no seu computador e o nível de protecção que as suas palavras-passe garantem.Clique em **Reparar** para modificar as palavras-passe fracas.

6. **Sumário**

   Aqui pode ver o resultado da operação.

## 19.2. Estado

Para ver o estado de vulnerabilidade actual e activar/desactivar a análise de vulnerabilidades automática, siga os seguintes passos:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Vulnerabilidade > Estado**.

A tabela mostrará as incidências que foram encontradas na ultima verificação de vulnerabilidade e o seu estado.Pode ver a acção levada a cabo para reparar cada uma das vulnerabilidades, caso tivesse havido alguma.Se a acção for **Nenhuma**, então a respectiva incidência não representa uma vulnerabilidade.

Importante

Para ser automaticamente notificado acerca das vulnerabilidades do seu sistema e aplicações, mantenha a **Análise Automática de Vulnerabilidades** activada.

Dependendo da incidencia, para reparar uma vulnerabilidade específica proceda da seguinte forma:

- Se estiverem disponiveis actualizações do Windows, clique em **Instalar** na coluna **Acções** para as instalar.
- Se uma aplicação estiver desactualizada, clique em **Mais informações** para saber a versão e seguir a hiperligação para a página de Internet do fornecedor a partir da qual pode instalar a versão mais recente dessa aplicação.
- Se uma conta de utilizador do Windows tem uma palavra-passe fraca, clique em **Ver & Corrigir**a para forçar o utilizador a mudar a palavra-passe da próxima vez que entrar no Windows ou então mude a palavra-passe directamente.Para obter uma palavra-passe forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).
- Se o recurso Execução Automática estiver activado no Windows, clique em **Corrigir** para o desactivar.

## 19.3. Definições

Para configurar as definições da verificação de vulnerabilidade automática, siga os seguintes passos:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Vulnerabilidade > Definições**.

3. Seleccione as caixas que correspondem às vulnerabilidades do sistema que deseja que sejam regularmente verificadas.
   - **Actualizações Críticas do Windows**
   - **Actualizações Regulares do Windows**
   - **Actualizações das Aplicações**
   - **Palavras-passe Fracas**
   - **Execução Automática**

Nota

Se limpar a a caixa correspondente a uma determinada vulnerabilidade, o BitDefender não o irá mais notificar acerca das incidências relacionadas.

# 20. Encriptação de Chat

O conteúdo das suas mensagens instantâneas deve permanecer entre si e a pessoa com quem conversa.Ao encriptar as suas conversas, tem a garantia que, se alguém tentar interceptá-las não conseguirá ler o conteúdo.

Por defeito, o BitDefender encripta todas as suas sessões de mensagens instantâneas desde que:

- O seu companheiro de conversação possui a versão BitDefender instalada que suporta a Encriptação de Conversas e esta está activada para a aplicação de conversação utilizada.
- Você ou o seu companheiro de conversação utilizam o Yahoo Messenger ou o Windows Live (MSN) Messenger.

Importante
BitDefender não irá encriptar uma conversação se o parceiro usar uma aplicação de chat web-based, tal como a Meebo, ou se um parceiro de conversação usar o Yahoo Messenger e o outro usar o Windows Leve (MSN).

Para configurar a encriptação de mensagens instantâneas:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Encriptação > Encriptação de Conversas**.

Nota
Pode configurar facilmente a encriptação de mensagens instantâneas para cada parceiro com a barra de ferramentas do BitDefender na janela de conversação.

Por defeito, a Encriptação de Mensagens Instantâneas está activada para o Yahoo Messenger e o Windows Live (MSN) Messenger.Pode escolher desactivar a encriptação de Mensagens Instantâneas para apenas uma aplicação de chat ou para todas.

São mostradas duas tabelas:

- **Exclusões da Encriptação** - lista os IDs dos utilizadores e o programa de IM associado para os quais a encriptação está desactivada.Para remover um contacto da lista , seleccione-o e clique no botão **Remover**.
- **Ligações Actuais** - lista as actuais ligações de mensagens (IDs dos utilizadores e o programa de IM associado) e se devem ou não ser encriptadas.Uma ligação poderá não ser encriptada pelas seguintes razões:
  - Desactivou explicitamente a encriptação para o respectivo contacto.

- O seu contacto não tem instalado uma versão do BitDefender que suporte a encriptação IM.

## 20.1. Desactivar a Encriptação para Utilizadores Específicos

Para desactivar a encriptação para um determinado utilizador, siga estes passos:

1. Clique no botão **Adicionar** para abrir a janela de configuração.
2. Insira no campo de edição o ID do utilizador do seu contacto.
3. Seleccione a aplicação de mensagens instântaneas associada ao contacto.
4. Clique em **OK**.

## 20.2. Barra de Ferramentas do BitDefender na Janela de Conversação

Pode configurar facilmente a encriptação de conversas instantâneas com a barra de ferramentas do BitDefender na janela de conversação.

A toolbar deve de estar no canto inferior direito da janela de chat. Procure aí o logo do BitDefender.

Nota
A toolbar indica que a conversação é encriptada ao mostrar um pequena chave ao pé do logo do BitDefender.

Ao clicar na toolbar do BitDefender são-lhe apresentadas as seguintes opções:

- **Desactivar permanentemente a encriptação para o `contacto`.**
- **Convidar `contacto` a usar a encriptação.** Para encriptar as suas conversações, o seu contacto deve de instalar o BitDefender e usar um programa de MI compatível.

# 21. Modo de Jogo / Portátil

O módulo do modo de Jogo / Portátil permite-lhe configurar os modos especiais de operação do BitDefender.

- O Modo de Jogo modifica temporariamente as definições da protecção de forma a minimizar o seu impacto no desempenho do sistema enquanto estiver a jogar.
- O Modo de Portátil evita que as atrefas agendadas sejam executadas quando o seu portátil esteja em modo de bateria de forma a economizar a mesma.
- Modo Silêncio modifica temporariamente as definições do produto para minimizar as interrupções quando vê filmes ou apresentações.

## 21.1. Modo de Jogo

O Modo de Jogo modifica temporariamente as definições da protecção de forma a minimizar o seu impacto no desempenho do sistema.Quando liga o Modo de Jogo, as seguintes definições são aplicadas:

- Todos os alertas e pop-ups do BitDefender são desactivados.
- O nível da protecção em tempo-real do BitDefender é definida como **Permissivo**.
- As actualizações não são executadas por defeito.

Nota

Para mudar esta definição, clique em Actualização >Configuração e limpe a caixa **Não actualizar se o Modo de Jogo estiver ligado**.

Por defeito, o BitDefender entra automaticamente em Modo de Jogo quando inicia um jogo da lista dos jogos conhecidos do BitDefender ou quando uma aplicação entra em Modo de ecrã inteiro.Pode entrar manualmente em Modo de Jogo usando a tecla de atalho predefinida `Ctrl+Alt+Shift+G`.É fortemente recomendado que saia do Modo de Jogo quando acaba de jogar (Pode usar a mesma tecla de atalho predefinida `Ctrl+Alt+Shift+G`).

Nota

Enquanto no Modo de Jogo, pode ver a letraG sobre o icone do BitDefender.

Para configurar o Modo Jogo:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá ao **Modo Jogo/Portátil > Modo Jogo**.

No topo da secção, pode ver o estado do Modo de Jogo.Pode clicar em **Modo Jogo está activado** ou **Modo Jogo está desactivado** para alterar o estado actual.

### 21.1.1. Configurar Modo de Jogo Automático

O Modo de Jogo Automático permite que o BitDefender entre automaticamente em Modo de Jogo quando um jogo é detectado.Pode configurar as seguintes opções:

- **Usar por defeito a lista de jogos do BitDefender** - para entrar automaticamente em Modo de Jogo quando inicia um jogo da lista dos jogos conhecidos do BitDefender.Para ver esta lista, clique em **Gerir Jogos** e depois em **Lista de Jogos**.
- **Acção em Ecrã Completo** - pode escolher activar automaticamente o Modo Jogo ou o Modo Silêncio sempre que uma aplicação fica em ecrã completo.
- **Perguntar se a aplicação em ecrã completo deve ser adicionada à lista de jogos** - para ser notificado para adicionar a nova aplicação à lista de jogos quando deixar o modo de ecrã inteiro.Ao adicionar uma nova aplicação à lista de jogos, da próxima vez que o jogar o BitDefender entrará automaticamente em Modo de Jogo.

Nota
Se não deseja que o BitDefender entre automaticamente em Modo Jogo, desmarque a caixa **Modo de Jogo Automático está activado**.

### 21.1.2. Gerir a Lista de Jogos

O BitDefender entra automaticamente em Modo de Jogo quando inicia uma aplicação que se encontra na lista de jogos.Para ver e gerira a lista de jogos, clique em **Gerir Jogos**.Uma nova janela irá aparecer.

Novas aplicações são adicionadas automaticamente à lista quando:

- Inicia um jogo da lista de jogos conhecidos do BitDefender.Para ver esta lista, clique em **Lista de Jogos**.
- Após siar do modo de ecrã inteiro, pode adicionar a aplicação à lista de jogos a partir da janela de notificação.

Se deseja descativar o Modo de Jogo Automático para uma determinada aplicação da lista, limpe a correspondente caixa de selecção.Deve de desactivar o Modo de Jogo Automático para as aplicações que regularmente entram em modo de ecrã inteiro, tais como os exploradores da Internet e os leitores de filmes.

Para gerir a lista de jogos, pode usar os botões colocados no topo da tabela:

- **Adicionar** - adiciona uma nova aplicação à lista de jogos.
- **Remover** - remove uma aplicação da lista de jogos.
- **Editar** - edita uma entrada existente na lista de jogos.

### 21.1.3. Adicionar ou Editar Jogos

Quando adicionar ou editar uma entrada da lista de jogos, aparecerá uma nova janela.

Clique em **Explorar** para seleccionar a aplicação e o caminho da mesma no campo de edição.

Se não quiser entrar automaticamente em Modo de Jogo quando a aplicação seleccionada é executada seleccione **Desactivar**.

Clique em **OK** para adicionar a entrada à lista de jogos.

### 21.1.4. Configurar as Definições do Modo de Jogo

Para configurar o comportamento das tarefas agendadas, use estas opções:

- **Activar este módulo para modificar os agendamentos das tarefas de análise Antivírus** - evita que a tarefa de análise agendada se execute enquanto o Modo de Jogo estiver ligado.Pode seleccionar uma das seguintes opções:

| Opção | Descrição |
|---|---|
| **Saltar Tarefa** | Não executar de todo a tarefa agendada. |
| **Adiar Tarefa** | Executa a tarefa imediatamente após sair do Modo de Jogo. |

### 21.1.5. Mudar a Tecla de Atalho do Modo de Jogo

Pode activar manualmente o Modo Jogo através de`Ctrl+Alt+Shift+G`tecla de atalho.Se deseja mudar a tecla de atalho, siga estes passos:

1. Clique em **Configuração Avançada**.Uma nova janela irá aparecer.
2. Por baixo da opção **Usar Tecla de Atalho** , defina a tecla de atalho desejada:
   - Escolha as teclas que deseja usar ao seleccionar uma das seguintes: Tecla Control (`Ctrl`), Tecla Shift (`Shift`) ou tecla Alternate (`Alt`).
   - No campo de edição, insira a letra correspondente à tecla que deseja usar.

   Por exemplo, de deseja usar as teclas de atalho `Ctrl+Alt+D` , deve seleccionar `Ctrl` e `Alt` e inserir `D`.

   Nota
   Remover a selecção junto a **Activar Tecla de Atalho** irá desactivar a tecla de atalho.

3. Clique em **Aplicar** para guardar as alterações.

## 21.2. Modo Portátil

O Modo de Portátil foi especialmente desenhado para os utilizadores de portáteis. O seu propósito é minimizar o impacto do BitDefender no consumo de energia enquanto o portátil estiver a funcionar a bateria.

Enquanto estiver em Modo de Portátil, as tarefas agendadas não serão levadas a cabo por defeito.

O BitDefender detecta quando o seu portátil está a funcionar a bateria e automaticamente entra em Modo de Portátil.De igual forma, O BitDefender sai automaticamente do Modo de Portátil quando detecta que o seu portátil já não está a funcionar a bateria.

Para configurar o Modo Portátil:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá ao **Modo Jogo/Portátil > Modo Portátil**.

Pode ver se o Modo de Portátil está ou não ligado.Se o Modo de Portátil está ligado, o BitDefender aplicará as definições configuradas para o portátil a funcionar a bateria.

### 21.2.1. Configurar Definições do Modo de Portátil

Para configurar o comportamento das tarefas agendadas, use estas opções:

- **Activar este módulo para modificar os agendamentos das tarefas de análise Antivírus** - evita que a tarefa de análise agendada se execute enquanto o Modo de Portátil estiver ligado.Pode seleccionar uma das seguintes opções:

| Opção | Descrição |
|---|---|
| **Saltar Tarefa** | Não executar de todo a tarefa agendada. |
| **Adiar Tarefa** | Executar a tarefa agendada assim que sair do Modo de Portátil. |

## 21.3. Modo Silêncio

O Modo Silêncio modifica temporariamente as definições da protecção de forma a minimizar o seu impacto no desempenho do sistema.Quando liga o Modo Silêncio, as seguintes definições são aplicadas:

- Todos os alertas e pop-ups do BitDefender são desactivados.
- As tarefas de análise agendadas são desactivadas por defeito.

Por defeito, o BitDefender activa automaticamente o Modo Silêncio sempre que vê um filme ou uma apresentação ou quando uma aplicação fica no modo de ecrã completo.É vivamente recomendado que saia do Modo Silêncio quando terminar o filme ou a apresentação.

Nota
No Modo Silêncio, pode ver uma ligeira modificação do pequeno ícone do BitDefender localizado junto ao relógio do seu computador.

Para configurar o Modo Silêncio:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá ao **Modo Jogo/Portátil > Modo Silêncio**.

No cimo da secção, pode ver o estado do Modo Silêncio.Pode clicar em **Modo Silêncio está activado** ou **Modo Silêncio está desactivado** para alterar o estado actual.

### 21.3.1. Configurar a Acção em Ecrã Completo

Pode configurar as seguintes opções:

- **Acção em Ecrã Completo** - pode escolher activar automaticamente o Modo Jogo ou o Modo Silêncio sempre que uma aplicação fica em ecrã completo.

Nota
Se não deseja que o BitDefender entre automaticamente em Modo Silêncio, desmarque a caixa de selecção **Acção em Ecrã Completo**.

### 21.3.2. Configurar as Definições do Modo Silêncio

Para configurar o comportamento das tarefas agendadas, use estas opções:

- **Activar este módulo para modificar os agendamentos das tarefas de análise Antivírus** - evita que a tarefa de análise agendada seja executada com o Modo Silêncio activado.Pode seleccionar uma das seguintes opções:

| Opção | Descrição |
|---|---|
| **Saltar Tarefa** | Não executar de todo a tarefa agendada. |
| **Adiar Tarefa** | Executar a tarefa agendada imediatamente após sair do Modo Silêncio. |

# 22. A Sua Rede

O módulo de rede permite-lhe gerir os produtos BitDefender instalados nos seus computadores em casa a partir de um só computador.Para aceder ao módulo de Rede Doméstica, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Intermédio
Abra o separador **Rede**.

Modo Avançado
Vá a **Rede Doméstica**.

Nota
Também pode adicionar um atalho a Meus Instrumentos.

Para poder gerir os produtos BitDefender instalados nos computadores de casa, siga os seguintes passos:

1. Activar a rede doméstica do BitDefender no seu computador.Defina o seu computador como Servidor.
2. Vá a cada computador que deseja gerir e adira-o à rede (defina a palavra-passe).Definir cada computador como Normal.
3. Volte para o seu computador e adicione os computadores que deseja gerir.

## 22.1. Activar a Rede BitDefender

Para activar a rede doméstica do BitDefender, siga os seguintes passos:

1. Clique em **Activar Rede**.Será notificado para configurar a palavra-passe de gestão de rede pessoal.
2. Insira a mesma palavra-passe em cada um dos campos editáveis.
3. Defina a função do computador na rede doméstica do BitDefender:
   - **Computador Servidor** - seleccione esta opção no computador que será utilizado para gerir os outros computadores.
   - **Computador Normal** - seleccione esta opção nos computadores que serão geridos pelo Computador Servidor.
4. Clique em **OK**.

Pode ver o nome do computador a aparecer no mapa de rede.

Aparece o botão **Desactivar Rede**.

## 22.2. Adicionar Computadores à Rede BitDefender

Todos os computadores serão automaticamente adicionados à rede se cumprir os seguintes requisitos:

- a rede doméstica BitDefender foi activada nele.
- a função foi definida como Computador Normal.
- a palavra-passe definida na activação da rede é a igual à definida no Computador Servidor.

Nota

No Modo Avançado, pode analisar a rede doméstica para encontrar os computadores que cumprem os requisitos clicando no botão **Auto-descobrir**.

Para adicionar manualmente um computador à rede doméstica BitDefender a partir do Computador Servidor, siga os seguintes passos:

1. Clique em **Adicionar Computador**.
2. Insira a palavra-passe de gestão rede pessoal e clique em **OK**.Uma nova janela irá aparecer.

   Pode ver a lista dos computadores na rede.O significado do ícone é o seguinte:

   Indica um computador on-line sem produtos BitDefender instalados.

   Indica um computador on-line com o BitDefender instalado.

   Indica um computador offline com o BitDefender instalado.
3. Faça uma das coisas seguintes:
   - Seleccione da lista o nome do computador a adicionar.
   - Insira o endereço IP ou o nome do computador a adicionar no campo correspondente.
4. Prima **Adicionar**.Será notificado para inserir a sua palavra-passe de gestão de rede pessoal do respectivo computador.
5. Insira a palavra-passe de gestão de rede pessoal configurada no respectivo computador.
6. Clique em **OK**.Se forneceu a palavra-passe correcta, a nome do computador seleccionado aparecerá no mapa de rede.

## 22.3. Gerir a Rede BitDefender

Uma vez que tenha criado com sucesso a sua rede pessoal BitDefender pode gerir todos os produtos BitDefender a partir de um único computador.

Se mover o curso do seu rato sobre um computador do mapa de rede, pode ver alguma informação acerca dele (nome, endereço IP, número de incidências que estão a afectar a segurança do sistema, o estado de registo do BitDefender).

Se clicar botão direito do rato sobre o nome de um computador no mapa de rede, pode ver todas as tarefas administrativas que pode levar a cabo no computador remoto.

- **Registar o BitDefender neste computador**

  Permite-lhe registar o BitDefender neste computador introduzindo a chave de licença.

- **Definir palavra-passe para acesso às definições num computador remoto**

  Permite-lhe criar uma password para restringir o acesso às definições do BitDefender nestes PC.

- **Executar tarefa de análise a-pedido**

  Permite-lhe executar uma análise a-pedido remota a partir de outro computador. Pode efectuar uma das seguintes tarefas: Análise Os Meus Documentos, Análise Completa do Sistema e Análise Minunciosa do Sistema.

- **Reparar incidências neste computador**

  Permite-lhe reparar as incidências que estão a afectar a segurança deste computador seguindo o assistente Reparar Incidências.

- **Ver Histórico/Eventos**

  Permite-lhe aceder ao módulo **Histórico&Eventos** do produto BitDefender instalado neste computador.

- **Actualizar Agora**

  Inicia o processo de Actualização para o produto BitDefender installado neste computador.

- **Definir com Servidor de Actualização desta rede**

  Permite-lhe definir este computador como servidor de actualizações para todos os produtos BitDefender instalados nos computadores desta rede.A utilização desta opção reduz o trafego de internet, porque apenas um computador vai necessitar de aceder a internet para descarregar as actualizações.

- **Remover o PC desta rede pessoal**

  Permite-lhe remover um PC da Rede.

Se o interface do BitDefender estiver no Modo Intermédio, pode executar várias tarefas em todos os computadores geridos ao mesmo tempo clicando nos respectivos botões.

- **Analisar Todos** - permite-lhe analisar ao mesmo tempo todos os computadores geridos.
- **Actualizar Todos** - permite-lhe actualizar ao mesmo tempo todos os computadores geridos.
- **Registar Todos** - permite-lhe registar ao mesmo tempo todos os computadores geridos.

Antes de levar a cabo uma tarefa num computador específico, será notificado para inserir a palavra-passe de gestão de rede pessoal local.Insira a palavra-passe de gestão rede pessoal e clique em **OK**.

Nota

Se planeia levar a cabo várias tarefas, seleccione **Não me mostrem mais esta mensagem durante esta sessão**.Ao seleccionar esta opção, não será notificado novamente pela palavra-passe durante esta sessão.

# 23. Actualização

Todos os dias é encontrado e identificado novo malware. Esta é a razão pela qual é muito importante manter o BitDefender actualizado com as últimas assinaturas de malware.

Se está ligado à Internet através de banda larga ou ADSL, o BitDefender executa esta operação sozinho. Quando liga o computador o BitDefender verifica se há novas actualizações e depois disso fá-lo a cada **hora** .

Se uma actualização é detectada, poderá ser notificado para confirmar a actualização ou a mesma é levada a cabo automaticamente, dependendo das definições automáticas da actualização.

O processo de actualização é executado "on the fly", o que significa que os ficheiros são substituidos progressivamente. Desta forma, o processo de actualização não afectará o funcionamento do produto e, ao mesmo tempo, exclui qualquer possibilidade de vulnerabilidade.

Importante
Para estar protegido contra as mais recentes ameaças mantenha a **Actualização Automática** activada.

As actualizações vêm em quatro “sabores”:

- **Actualizações para a engenharia Antivírus** - à medida que vão surgindo novas ameaças, os ficheiros que contêm assinaturas de vírus têm de ser actualizados para assegurar a protecção actualizada permanente contra os vírus. Esta actualização é também conhecida como **Virus Definitions Update**.
- **Actualizações para o motor de Antispyware** - novas assinaturas de spyware serão adicionadas à base de dados. Esta actualização é também conhecida como **Antispyware Update**.
- **Actualizações do produto** - quando é lançada uma nova versão do produto, são introduzidas novas configurações e técnicas de verificação, com o objectivo de melhorar o desempenho do produto. Esta actualização é também conhecida como **Product Update**.

## 23.1. Efectuar uma Actualização

A actualização automática pode também ser feita a qualquer altura que deseje premindo o botão **Actualizar Agora**. Esta actualização é também conhecida como **actualização a pedido do utilizador**.

Para actualizar o BitDefender, consoante o modo do interface, proceda da seguinte forma:

**Modo Básico**
Clique no ícone **Actualizar Agora** na área Proteja o seu PC.

**Modo Intermédio**
Abra o separador **Segurança** e clique em **Actualizar Agora**, nas Tarefas Rápidas, no lado esquerdo da janela.

**Modo Avançado**
Vá a **Actualizar > Actualizar**.

O módulo de **Actualização** estabelece ligação ao servidor de actualizações do BitDefender e verificará se há actualizações disponíveis. Se detectar uma actualização, dependendo das opções definidas na secção Opções da Actualização Manual, ser-lhe-á solicitada a confirmação para a actualização ou a actualização será feita automaticamente.

Importante
Poderá ser necessário reiniciar o computador quando a actualização tiver terminado. Recomendamos que o faça o quanto antes.

Nota
Se está ligado à Internet através de uma ligação dial-up, então é uma boa ideia adquirir o hábito de actualizar o Bitdefender a seu pedido.Para mais informação, por favor consulte o "*Como Actualizar o BitDefender numa Ligação à Internet Lenta*" (p. 126).

## 23.2. Configurar Definições de Actualização

As actualizações podem ser executadas através da rede local, da Internet, directamente ou através de um servidor proxy.Por defeito, o BitDefender verificará as actualizações a cada hora, via Internet, e instalará as que estejam disponíveis sem o avisar.

Para configurar as definições de actualização:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Actualização > Definições**.
3. Configure as definições como necessário.Para saber o que uma opção faz, mantenha o rato sobre a mesma e leia a descripção apresentada no fundo da janela.
4. Prima **Aplicar** para guardar as alterações.

Para aplicar as configurações por defeito, clique em **Por Defeito**.

As configurações da actualização estão agrupadas em 4 categorias (**Configuração da Localização da Actualização**, **Configuração de actualização automática**,

**Configuração de Actualização Manual** e **Configuração Avançada**). Cada categoria será descrita separadamente.

### 23.2.1. Configuração da Localização da Actualização

Para definir a localização da actualização, use as opções da categoria **Configuração da Localização da Actualização** .

Nota

Configure estas definições apenas se estiver ligado a uma rede local que armazena localmente as assinaturas de malware do BitDefender ou se liga à Internet através de um servidor proxy.

Para actualizações mais rápidas e fiáveis, pode configurar dois locais de actualização: um **Local primário de actualização** e um **Local alternativo de actualização**. Por defeito estas localizações são iguais:`http://upgrade.bitdefender.com`.

Para modificar um dos locais de actualização, insira o URL do local mirror no campo **URL** que corresponde ao novo local para o qual deseja mudar.

Nota

Recomendamos que defini como local primário de actualização o local mirror e deixar o local alternativo de actualização como está, como um plano de backup em caso do local mirror ficar indisponível.

No caso em que a empresa usa um servidor proxy para se ligar à Internet, seleccione **Usar proxy** de depois clique em **Gerir proxies** para configurar as definições do proxy.Para mais informações, por favor consulte"Definições de Ligação" (p. 53)

### 23.2.2. Configurar Actualização Automática

Para configurar o processo de actualização automática do BitDefender, use as opções na categoria **Configuração Actualização Automática** .

Pode definir o intervalo entre duas verificações consecutivas de actualizações no campo **Intervalo de Tempo**. Por defeito, o intervalo de tempo da actualização é de 1 hora.

Para definir como é que o processo de actualização automática tem de ser feito, seleccione uma das seguintes opções:

- **Actualização silenciosa** - O BitDefender faz automaticamente o download e a implementação da actualização.
- **Avisar antes de fazer download das actualizações** - cada vez que uma actualização está disponível, será consultado antes do download ser feito.
- **Avisar antes de instalar actualizações** - cada vez que uma actualização for descarregada, será consultado antes da sua instalação ser feita.

### 23.2.3. Configurar Actualização Manual

Para definir como a actualização manual (actualização a pedido do utilizador) deve ser executada, seleccione uma das seguintes opções na categoria **Configuração Actualização Manual**:

- **Actualização silenciosa** - a actualização manual será feita em segundo plano automaticamente.
- **Avisar antes de fazer download das actualizações** - cada vez que uma actualização está disponível, será consultado antes do download ser feito.

### 23.2.4. Configuração Avançada

Para evitar que o processo de actualização do BitDefender interfira com o seu trabalho, configure as opções na categoria **Configuração Avançada**:

- **Esperar pelo reiniciar, em vez se o solicitar** - Se uma actualização requer um reiniciar, o produto continuará a funcionar com os antigos ficheiros até que o sistema reinicie. Ao utilizador não lhe será solicitado que o reinicie, logo o processo de actualização do BitDefender não interferirá com o trabalho do utilizador.
- **Não actualizar se a análise estiver a decorrer** - O BitDefender não vai actualizar se estiver a decorrer uma análise. Desta forma, o processo de actualização do BitDefender não vai interferir com as tarefas de análise.

  Nota
  Se o BitDefender for actualizado enquanto a análise estiver a decorrer, o processo de análise será interrompido.

- **Não actualizar se o Modo Jogo estiver activado** - O BitDefender não actualizará se o Modo Jogo estiver activado.Desta forma, poderá minimizar a influência do produto no desempenho do sistema durante os jogos.
- **Activar partilha de actualizações** - Se quiser minimizar o impacto do tráfego de rede no desempenho do sistema durante as actualizações, utilize a opção de partilha de actualizações.
- **Transferir ficheiros do BitDefender deste PC** - O BitDefender permite-lhe partilhar as mais recentes assinaturas antivírus disponíveis no seu computador com outros utilizadores do BitDefender.

Como

# 24. Como Posso Analisar Ficheiros e Pastas?

A análise é simples e flexível com o BitDefender.Há várias formas de definir o BitDefender para analisar ficheiros e pastas em busca de vírus e outro malware:

- Usar o Menu Contextual do Windows
- Usar Tarefas de Análise
- Usando a Barra de Actividade da Análise

Uma vez que inicie uma análise, o assistente de Análise de Antivírus irá aparecer e guiá-lo através do processo de análise.Para mais informações sobre este assistente, por favor consulte o "*Assistente de Análise Antivírus*" (p. 65).

Nota

Para saber como utilizar o BitDefender para analisar no Modo de Segurança do Windows, consulte "*Como Posso Analisar o Computador no Modo de Segurança?*" (p. 133).

## 24.1. Usar o Menu Contextual do Windows

Esta é a forma mais fácil e recomendada para analisar um ficheiro ou pasta no seu computador.Clique com o botão direito do rato sobre o objecto que pretende analisar e seleccione no menu **Analisar com o BitDefender**.Siga o assistente de Análise Antivírus para completar a análise.

Situações tipicas em que deve de usar este método de análise são as seguintes:

- Suspeita que um determinado ficheiro ou pasta está infectado.
- Sempre que descarrega da Internet ficheiros que julga serem perigosos.
- Quer analisar uma partilha de rede antes de copiar os ficheiros para o seu computador.

## 24.2. Usar Tarefas de Análise

Se deseja analisar o seu computador ou determinadas pastas regularmente, deve de considerar usar as tarefas de análise.Tarefas de análise indicam ao BitDefender as áreas a analisar, e que opções ou acções de análise devem ser usadas. Mais ainda, pode Agendá-las para serem levadas a cabo numa base regular ou numa determinada altura.

Para analisar o seu computador usando as tarefas de análise, deve de abrir o interface BitDefender e levar a cabo a tarefa de análise desejada.Dependendo do modo do interface do utilizador, são várias as etapas a seguir para executar o scan.

### Levar a cabo Tarefas de Análise em Modo Básico

No Modo Básico, pode executar várias tarefas de análise pré-configuradas.Clique no botão **Segurança** e escolha a tarefa de análise pretendida.Siga o assistente de Análise Antivírus para completar a análise.

### Realizar Tarefas de Análise em Modo Intermédio

Na Modo Intermédio, pode executar várias tarefas de análise pré-configuradas. Também pode configurar e executar tarefas de análise personalizadas especificando as localizações nas opções de análise.Siga estes passos para realizar uma tarefa de análise em Modo Intermédio:

1. Clique na barra **Segurança** .
2. No lado esquerdo da área de Tarefas Rápidas, clique em **Análise Minuciosa ao Sistema** e escolha a tarefa de análise pretendida.Para configurar e executar uma anákise personalizada, clique em **Análise Personalizada**.
3. Siga o assistente de Análise Antivírus para completar a análise.Se preferir executar uma análise personalizada, deverá completar o assistente de Análise Personalizada.

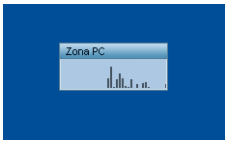
### Executar Tarefas de Análise em Modo Avançado

No Modo Avançado, pode levar a cabo todas as tarefas de análise pré-configuradas, e também alterar as suas opções. Mais ainda, pode criar as suas próprias tarefas de análise se deseja analisar locais específicos no seu computador.Siga estes passos para realizar uma tarefa de análise em Modo Avançado:

1. Clique em **Antivirus** do lado esquerdo do menu.
2. Clique na barra **Analisar**Aqui pode encontrar um conjunto de tarefas de análise pré-configuradas e pode criar as suas próprias tarefas de análise.
3. Faça duplo-clique na tarefa de análise que quer executar.
4. Siga o assistente de Análise Antivírus para completar a análise.

## 24.3. Usando a Barra de Actividade da Análise

A **Barra de Actividade da Análise** é um gráfico de visualização da actividade de verificação no seu sistema.Esta pequena janela, por defeito, está apenas disponível no Modo Avançado.



Barra de Actividade da Análise

Pode usar a barra de actividade da análise para analisar rapidamente ficheiros e pastas.Drag & drop o ficheiro ou pasta a ser analisado para a

barra de actividade da análise.Siga o assistente de Análise Antivírus para completar a análise.

Nota
Para mais informação, por favor consulte o “*Barra de Actividade da Análise*” (p. 19).

# 25. Como Posso Criar Uma Tarefa de Análise Personalizada?

Para criar uma tarefa de análise, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Intermédio

Abra o separador **Segurança** e clique em **Personalizar Análise**, nas Tarefas Rápidas, no lado esquerdo da janela.

Vai aparecer um assistente para ajudar a criar uma tarefa de análise.Pode navegar pelo assistente utilizando os botões **Seguinte** e **Retroceder**.Para sair do assistente, clique em **Cancelar**.

1. **Bem-vindo**
2. **Seleccionar Alvo**

   Clique em **Adicionar Alvo** para seleccionar os ficheiros ou as pastas a analisar.

   Clique em **Configuração Avançada**.No separador **Apresentação**, configure as opções de análise movendo o cursor na barra deslizante.Se desejar configurar detalhadamente as opções de análise, clique em **Personalizar**.Abra o separador **Agendar** para escolher quando a tarefa deve ser executada.
3. **Terminar**

   Aqui pode inserir o nome da tarefa e, opcionalmente, adicionar a análise na área das Tarefas Rápidas.

   Clique em **Iniciar Análise** para criar a tarefa e iniciar o assistente de análise.

Modo Avançado

1. Vá a **Antivírus > Análise de Vírus**.
2. Clique em **Nova Tarefa**Aparecerá uma nova janela.

   Nota

   Também pode clicar com o botão direito numa tarefa de análise predefinida, como a **Análise Minuciosa ao Sistema** e escolher **Clonar Tarefa**.Isto é útil na criação de novas tarefas, pois pode modificar as definições da tarefa duplicada.
3. No separador **Apresentação**, introduza o nome da tarefa e configure as opções de análise movendo o cursor na barra deslizante.

Se desejar configurar detalhadamente as opções de análise, clique em **Personalizar**.

4. Vá ao separador **Caminhos** para seleccionar o alvo da análise. Clique em **Adicionar Itens** para seleccionar os ficheiros ou as pastas a analisar.
5. Abra o separador **Agendar** para escolher quando a tarefa deve ser executada.
6. Clique em **Ok** para guardar a tarefa.A nova tarefa vai aparecer nas tarefas definidas pelo Utilizador e pode ser editada, removida ou executada em qualquer momento a partir desta janela.

# 26. Como Posso Agendar uma Análise ao Computador?

Analisar o seu computador periodicamente é a melhor prática para o manter livre de malware. O BitDefender permite-lhe agendar as tarefas de análise de forma a poder analisar automaticamente o seu computador.

Para agendar o BitDefender de forma a analisar o seu computador, siga estes passos:

1. Abrir o BitDefender.
2. Dependendo do modo de interface do utilizador, proceda da seguinte forma:

   Modo Intermédio
   Abra o separador **Segurança** e clique em **Configurar o Antivírus**, nas Tarefas Rápidas, no lado esquerdo da janela.

   Modo Avançado
   Clique em **Antivirus** do lado esquerdo do menu.
3. Clique na barra **Analisar**Aqui pode encontrar um conjunto de tarefas de análise pré-configuradas e pode criar as suas próprias tarefas de análise.

   - As tarefas de sistema estão disponíveis e podem ser levadas a cabo em qualquer conta de utilizador Windows.
   - Tarefas de utilizador estão apenas disponíveis para o mesmo e só podem ser usadas por quem as criou.

   Estas são as análises pré-configuradas que pode agendar:

   **Análise Completa**
   Analisa todo o sistema, excepto arquivos.Na configuração por defeito, analisa todos os tipos de malware excepto rootkits.

   **Análise Rápida**
   A Análise Rápida utiliza a análise nas nuvens para detectar malware em execução no seu sistema.Normalmente, a realização de uma Análise Rápida demora menos de um minuto e utiliza uma facção dos recursos do sistema necessários para uma análise de vírus normal.

   **Análise Autologon**
   Analisar os itens que são executados quando o utilizador entra no Windows.Para usar esta tarefa, deve de agendá-la para ser levada a cabo durante o iniciar do sistema.Por defeito, a análise ao logon está desactivada.

   **Análise Minuciosa**
   Analisa todo o sistema.Na configuração por defeito, faz uma nálise em busca de todo o tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.

**Os meus documentos**

Use esta tarefa para analisar pastas de utilizadores actuais: `Os Meus Documentos`, `Ambiente de Trabalho` e `StartUp`. Isto irá assegurar a segurança dos seus documentos, uma área de trabalho segura e aplicações limpas a serem executadas no arranque.

Se nenhuma destas tarefas de análise servir, pode criar uma nova tarefa de análise que pode depois agendar para ser levada a cabo quando quiser.

4. Clique com o botão-direito na tarefa de análise desejada e seleccione **Agendar**.Uma nova janela irá aparecer.
5. Agende a tarefa para ser levada a cabo quando quiser:
   - Para levar a cabo a tarefa de análise uma só vez, seleccione **Uma só vez** e especifique a data e hora de inicio.
   - Para levar a cabo a tarefa de análise após o iniciar do sistema, seleccione **No iniciar do sistema**.Pode definir quanto tempo após o iniciar do sistema a tarefa deve de ser iniciada.
   - Para levar a cabo a tarefa de análise numa base regular, seleccione **Periodicamente** e especifique a frequência e a data e hora de inicio.

   Nota

   Por exemplo, para analisar o seu computador cada Sábado às 2 PM, deve de configurar o agendar da seguinte forma:

   a. Seleccione **Periodicamente**.

   b. No campo **A cada**, insira 1 e depois seleccione **semanas** do menu.Desta forma, a tarefa é levada a cabo a cada semana.

   c. Defina como data de início o primeiro Sábado a aparecer.

   d. Defina como hora de início `2:00:00 AM`.

6. Clique em **OK** para guardar o agendamento.A tarefa de análise irá ser levada a cabo automaticamente de acordo com o agendamento que definiu.Se o computador estiver desligado durante o momento do agendamento, a tarefa será levada a cabo da próxima vez que iniciar o seu computador.

# 27. Como Posso Actualizar o BitDefender Através de um Proxy?

Normalmente, o BitDefender detecta e importa automaticamente as definições proxy do seu sistema.Se estiver ligado à Internet através de um servidor proxy, poderá ter de procurar as definições proxy e configurar o BitDefender correctamente.Para saber como fazer isto, consulte "*Como Posso Encontrar as Minhas Definições de Proxy?*" (p. 147).

Depois de encontrar as definições de proxy, siga os seguintes passos:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Geral > Definições**.
3. Clique em **Definições Proxy** na secção**Definições da Ligação**.
4. Insira as definições de proxy nos respectivos campos.
5. Clique em **OK**.

Nota

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção "*Apoio*" (p. 138).

# 28. Como Posso Fazer o Upgrade para Outro Produto do BitDefender 2011?

Com o BitDefender 2011 pode fazer facilmente o upgrade de um produto BitDefender 2011 para outro.

Imaginemos a seguinte situação: tem vindo a utilizar o BitDefender Antivirus Pro 2011 2011 há já algum tempo e decidiu recentemente mudar para o BitDefender Total Security 2011, com todos os recursos adicionais que este oferece.

Tudo o tem de fazer é adquirir uma chave de licença para o BitDefender 2011 que quer fazer o upgrade e introduza-a na janela de registo do produto BitDefender 2011 que está actualmente a utilizar.

Siga estes passos:

1. Abrir o BitDefender.
2. Clique na hiperligação **Informação de Licença** no fundo da janela.A janela de registo irá aparecer.
3. Introduza a chave de registo e clique em **Registar Agora**.
4. O BitDefender irá informar que a chave de licença destina-se a um produto diferente e dará a opção de instalá-lo.Clique na respectiva hiperligação e siga o procedimento de três passos para efectuar o upgrade.
   a. **Confirmar Acção**
   b. **Upgrade em curso**

      Aguarde que o BitDefender conclua o processo de upgrade.Isto irá demorar alguns minutos.
   c. **Upgrade concluído**

      O processo foi concluído. Poderá ser necessário reiniciar o sistema.

# Troubleshooting e Obter Ajuda

# 29. Solução de problemas

Este capítulo apresenta alguns dos problemas que poderá encontrar ao utilizar o BitDefender e as possíveis soluções.A maioria destes problemas pode ser resolvida com a configuração correcta das definições do produto.

Se não conseguir encontrar o seu problema aqui, ou se as soluções apresentadas não resolvem o seu problema, pode contactar os representantes do apoio técnico da BitDefender como mostrado no capítulo "*Apoio*" (p. 138).

## 29.1. Problemas de Instalação

Este artigo vai ajuda-lo a solucionar os problemas de instalação mais comums do BitDefender.Estes problemas podem ser agrupados nas seguintes categorias:

- Erros de validação de Instalação: o assistente de configuração não pode ser executado devido a condições específicas do seu sistema.
- Instalações falhadas: iniciou a instalação do assistente de configuração, mas não foi concluída com êxito.

### 29.1.1. Erros de Validação da Instalação

Quando você iniciar o assistente de instalação, um número de condições são verificadas para validar se a instalação pode ser iniciada.A seguinte tabela apresenta as validadções e erros das instalações mais comuns, bem como o ajuda a solucioná-las.

| Erro | Descrição&Solução |
|---|---|
| Não possui privilégios suficientes para instalar o programa. | Para poder executar o assistente de instalação e instalar o BitDefender necessita de provilégios de administrador.Faça uma das coisas seguintes:<br>● Entre com uma conta de administrador do Windows e execute de novo o assistente de instalação.<br>● Clique com o botão-direito no ficheiro de instalação **Executar como**.Digite no sistema o nome de utilizador e a palavra-passe de uma conta de administrador do Windows. |
| O instalador detectou uma versão anterior do produto BitDefender que não foi devidamente desinstalada. | O BitDefender foi anteriormente instalado no seu sistema, mas a instalação não foi completamente removida. Esta condição bloqueia uma nova instalação do BitDefender. |

| Erro | Descrição&Solução |
|---|---|
| | Para superar este erro e instalar o BitDefender, siga estes passos:<br>1. Vá a www.bitdefender.com/uninstall e descarregue a ferramenta de desinstalação para o seu computador.<br>2. Execute a ferramenta de desinstalação com direitos de administrador.<br>3. Reinicie o seu computador.<br>4. Volte a iniciar o assistente de instalação para reinstalar o BitDefender. |
| O produto BitDefender não é compatível com o seu sistema operativo. | Está a tentar instalar o BitDefender num sistema operativo nao suportado.Por favor consulte o *"Requisitos de Sistema"* (p. 2) para saber em que sistemas operativos pode instalar no BitDefender.<br>Se o seu sistema operativo é o Windows XP com o Service Pack 1 ou sem nenhum service pack, pode instalar o Service Pack 2 ou superior e em seguida executar novamente o assistente de instalação. |
| O ficheiro de instalação foi concebido para um diferente tipo de processador. | Se receber esse erro, significa que está a tentar executar uma versão incorreta do ficheiro de instalação.Existem duas versões do ficheiro de instalação do BitDefender: um para processadores 32-bit e outro para processadores 64-bit.<br>Para se certificar que tem a versão correta para o seu sistema, faça o download do ficheiro de instalação diretamente do site www.bitdefender.com. |

### 29.1.2. Falha na Instalação

Existem várias possibilidades para instalação falhar:

- Durante a instalação, aparece uma imagem de erro.Pode ser solicitado que cancele a instalação ou fornecido um botão para executar a ferramenta de desinstalação que irá limpar o sistema.

**Nota**
Imediatamente após iniciar a instalação, pode ser informado de que não possui espaço livre suficiente no disco rígido para instalar o BitDefender. Nesse caso, liberte o espaço necessário em disco na partição onde quer que o BitDefender seja instalado e depois continue ou recomece a instalação.

- A instalação trava e possivelmente, o seu sistema bloqueia.Apenas o reiniciar restaura a responsividade do sistema.
- A instalação foi concluída, mas não pode utilizar algumas ou todas as funções BitDefender.

Para detectar o problema de uma falha na instalação e instalar o BitDefender, siga os seguintes passos:

1. **Limpe o sistema depois da falha de instalação.** Se a instalação falhar, algumas chaves de registo e ficheiros do BitDefender poderão manter-se no seu sistema. Podem também afectar o desempenho e a estabilidade do sistema. Por isso deve removê-los antes de tentar instalar o produto novamente.

   Se for este o caso, a solução mais fácil é remover totalmente o BitDefender do sistema e, depois, reinstalá-lo.Para mais informação, por favor consulte o "*Como Posso Remover Totalmente o BitDefender?*" (p. 147).

2. **Verificar causas possíveis para a instalação ter falhado.** Antes de avançar para reinstalar o produto, verifique e remova possíveis condições que podem ter causado a falha da instalação:

   a. Verifique se tem qualquer outra solução de segurança instalada na medida em que possam interferir no funcionamento normal do BitDefender. Se for este o caso, recomendamos que remova todas as outras soluções de segurança e reinstale BitDefender.

   b. Também deve verificar se seu sistema está infectado.Faça uma das coisas seguintes:

      - Utilize o BitDefender Rescue CD para analisar seu computador e remover quaisquer ameaças existentes.Para mais informação, por favor consulte o "*CD de Emergência BitDefender*" (p. 129).
      - Abra a janela do Internet Explorer, vá a www.bitdefender.com e execute a análise online (clique no botão **Analise Agora**).

3. Volte a tentar instalar o BitDefender.É recomendado que descarregue e execute a ultima versão do ficheiro de instalação em www.bitdefender.com.
4. Se a instalação falhar, contacte a BitDefender para suporte, como descrito na secção "*Apoio*" (p. 138).

## 29.2. O meu sistema parece estar lento

Normalmente, após a instalação de um software de segurança, o sistema poderá abrandar ligeiramente, o que é, até um certo nível, normal.

Se notar um abrandamento significativo, este problema pode dever-se às seguintes razões:

- **O BitDefender não é o único programa de segurança instalada no sistema.**

Apesar de o BitDefender procurar e remover os programas de segurança encontrados durante a instalação, é recomendado que remova todos os outros programas antivírus utilizados antes de instalar o BitDefender.Para mais informação, por favor consulte o "*Como Posso Remover Outras Soluções de Segurança?*" (p. 145).

- **Não estão cumpridos os Requisitos Mínimos do Sistema para executar o BitDefender.**

  Se o seu computador não cumprir os Requisitos Mínimos do Sistema, ficará lento, especialmente se estiver a executar muitas aplicações ao mesmo tempo.Para mais informação, por favor consulte o "*Requisitos Minímos do Sistema*" (p. 2).

- **As unidades do seu disco rígido estão demasiado fragmentadas.**

  A fragmentação dos ficheiros abranda o acesso aos ficheiros e diminui o desempenho do sistema.

  Para desfragmentar o seu disco com o sistema operativo do Windows, siga o caminho a partir do menu Iniciar: **Iniciar → Todos os Programas → Acessórios → Ferramentas do Sistema → Desfragmentador de Disco**.

## 29.3. A Análise Não Inicia

Este tipo de problema pode ter duas causas principais:

- **Uma instalação anterior do BitDefender que não foi totalmente removida ou uma instalação do BitDefender mal sucedida**.

  Se for este o caso, a solução mais fácil é remover totalmente o BitDefender do sistema e, depois, reinstalá-lo.Para mais informação, por favor consulte o "*Como Posso Remover Totalmente o BitDefender?*" (p. 147).

- **O BitDefender não é a única solução de segurança instalada no seu sistema**.

  Neste caso, siga os passos seguintes:

  1. Remover a outra solução de segurança.Para mais informação, por favor consulte o "*Como Posso Remover Outras Soluções de Segurança?*" (p. 145).
  2. Remover o BitDefender totalmente do sistema.
  3. Reinstalar o BitDefender no sistema.

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção "*Apoio*" (p. 138).

## 29.4. Já Não Consigo Utilizar uma Aplicação

Este problema ocorre quando está a tentar utilizar um programa que estava a funcionar normalmente antes de instalar o BitDefender.

Poderá encontrar uma das seguintes situações:

- Poderá receber uma mensagem do BitDefender a informar que o programa está a tentar modificar o sistema.
- Pode receber uma mensagem de erro do programa que está a tentar utilizar.

Este tipo de situação ocorre quando o módulo de Controlo Activo de Vírus classifica erradamente algumas aplicações como maliciosas.

O Controlo de Vírus Activo é um módulo do BitDefender que monitoriza constantemente as aplicações executadas no seu sistema e denuncia o comportamento potencialmente malicioso.Como este recurso é baseado num sistema heurístico, poderá haver casos em que as aplicações legítimas são denunciadas pelo Controlo Activo de Vírus.

Quando isto acontece, pode excluir a respectiva aplicação da monitorização do Controlo Activo de Vírus.

Para adicionar o programa à lista de exclusões, siga os seguintes passos:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Antivírus > Escudo**.
3. Clique em **Configuração Avançada**.
4. Na nova janela, abra o separador **Exclusões**, clique no botão **Adicionar** e procure a localização do ficheiro .exe do programa (normalmente localizado na pasta `C:\Programa`).
5. Clique em **OK** para guardar as alterações e fechar a janela.
6. Feche a janela do BitDefender e confirme se o problema ainda persiste.

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção “*Apoio*” (p. 138).

## 29.5. Como Actualizar o BitDefender numa Ligação à Internet Lenta

Se tiver uma ligação à Internet lenta (por exemplo, ligação telefónica), poderão ocorrer erros durante o processo de actualização.

Para manter o seu sistema actualizado com as mais recentes assinaturas de malware BitDefender, siga os seguintes passos:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Actualização > Definições**.

3. Em **Definições da Actualização Manual**, seleccione **Perguntar antes de transferir actualizações**.
4. Clique em **Aplicar** e abra o separador **Actualizar**.
5. Clique em **Actualizar Agora** e aparecerá uma nova janela.
6. Seleccione apenas **Actualizações das assinaturas** e clique em **Ok**.
7. O BitDefender vai transferir e instalar apenas as actualizações das assinaturas de malware.

## 29.6. O Meu Computador Não Está Ligado à Internet. Como Posso Actualizar o BitDefender?

Se o seu computador não estiver ligado à Internet, tem de transferir manualmente as actualizações para um computador com acesso à Internet e, depois, transferi-las para o seu computador com um dispositivo amovível, por exemplo, um USB.

Siga estes passos:

1. Num computador com acesso à Internet, abra o navegador da Internet e vá a:

   www.bitdefender.com/site/view/Desktop-Products-Updates.html

2. Na coluna **Actualização Manual**, clique na hiperligação que corresponde ao seu produto e à arquitectura do sistema.Se não sabe se a versão do seu Windows é de 32 ou 64 bits, consulte "*Estou a Utilizar uma Versão de 32 ou 64 Bit do Windows?*" (p. 146).
3. Guarde o ficheiro com o nome `weekly.exe` no sistema.
4. Mova o ficheiro transferido para um dispositivo amovível, tal como uma unidade USB, e depois para o seu computador.
5. Faça duplo clique no ficheiro e siga os passos do assistente.

## 29.7. Os serviços BitDefender não estão a responder

Este artigo ajuda-o a troubleshoot os erros de*Os Serviços BitDefender não estão a responder*.Pode encontrar esse erro da seguinte forma:

- O icon BitDefender na Barra de Notificação está a cinzenta e um pop-up informa que os serviços do BitDefender não estão a responder.
- A janela do BitDefender indica que os serviços do BitDefender não estão a responder.

O erro pode ter ocorrido devido a um dos seguintes factores:

- Está a ser instalada uma actualização importante.
- problemas temporários de comunicação entre os serviços da BitDefender.

- alguns dos serviços da BitDefender estão parados.
- Outras soluções de segurança em execução no seu computador, ao mesmo tempo que o BitDefender.
- Os vírus no seu sistema afectam o funcionamento normal do BitDefender.

Para solucionar este erro, tente estas soluções:

1. Espere uns momentos e verifique se existe alguma alteração.Este erro pode ser temporário.
2. Reinicie o computador e aguarde alguns momentos até o BitDefender iniciar. Abra o BitDefender e veja se o erro se mantém.Reiniciar o computador normalmente resolve o problema.
3. Verifique se tem qualquer outra solução de segurança instalada na medida em que possam interferir no funcionamento normal do BitDefender. Se for este o caso, recomendamos que remova todas as outras soluções de segurança e reinstale BitDefender.
4. Se o erro persistir, pode haver um problema mais grave (por exemplo, pode estar infectado com um vírus que interfere com o BitDefender).Por favor contacte a BitDefender para suporte, como descrito na secção “*Apoio*” (p. 138).

## 29.8. A Desinstalação do BitDefender Falhou

Este artigo ajuda-o a resolver erros que possam ocorrer quando remover o BitDefender.Há duas situações possíveis:

- Durante a remoção, aparece uma imagem de erro.O ecrã apresenta um botão para executar uma ferramenta de desinstalação que irá limpar o sistema.
- A remoção trava e possivelmente, o seu sistema bloqueia.Clique em **Cancelar** para abortar a desinstalação. Se isso não funcionar, reinicie o sistema.

Se a desinstalação falhar, algumas chaves de registo e ficheiros do BitDefender poderão manter-se no seu sistema. Esses resquícios podem impedir uma nova instalação do BitDefender. Podem também afectar o desempenho e a estabilidade do sistema.Para remover completamente o BitDefender do seu sistema, deverá executar a ferramenta de desinstalação.

Para mais informação, por favor consulte o “*Como Posso Remover Totalmente o BitDefender?*” (p. 147).

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção “*Apoio*” (p. 138).

# 30. Remover Malware do Sistema

O malware pode afectar o seu sistema de várias formas e a actuação do BitDefender depende do tipo de ataque por malware.Como os vírus alteram frequentemente o modo de acção, é difícil estabelecer um padrão com base no comportamento e nas acções.

Há situações em que o BitDefender não consegue remover automaticamente a infecção por malware do seu sistema.Nestes casos, a sua intervenção é necessária.

Se não conseguir encontrar o seu problema aqui, ou se as soluções apresentadas não resolvem o seu problema, pode contactar os representantes do apoio técnico da BitDefender como mostrado no capítulo “*Apoio*” (p. 138).

## 30.1. CD de Emergência BitDefender

**CD de Recuperação do BitDefender** é um recurso incluído na maioria dos CDs de instalação do BitDefender que permite analisar e desinfectar todos os discos rígidos existentes antes de o seu sistema operativo arrancar.Também pode ajudar a guardar dados do seu computador Windows em risco num dispositivo amovível.

Se não possuir um CD de Recuperação do BitDefender, pode transferir na forma de imagem ISO a partir do seguinte local:

http://download.bitdefender.com/rescue_cd/

Transfira o ficheiro .iso e grave-o num CD ou DVD com uma ferramenta à sua escolha.

### Analisar o Sistema com o CD de Recuperação do BitDefender

Para analisar o seu sistema com o CD de Recuperação do BitDefender, siga os seguintes passos:

1. Configure a BIOS do seu computador para desligar o CD.
2. Coloque o CD na unidade e reinicie o computador.
3. Aguarde que o ecrã do BitDefender apareça e seleccione **Iniciar CD de Recuperação do BitDefender** no idioma preferido.
4. Aguarde que o processo de arranque termine. Poderá demorar algum tempo.
5. Assim que estiver concluído o processo de arranque, as assinaturas do BitDefender são automaticamente actualizadas e é iniciada uma análise a todas as partições do disco rígido detectadas.

### Guardar Dados com o CD de Recuperação do BitDefender

vamos partir do principio que não consegue arrancar o seu PC em Windows PC devido a incidências desconhecidas. Ao mesmo tempo, você necessita desesperadamente de aceder a alguma informação importante do seu computador.

Eis aqui uma situação em que o CD de Emergência BitDefender se revela extremamente útil.

Para guardar os seus dados do computador para um dispositivo amovível, tal como um dispositivo USB, siga os seguintes passos:

1. Configure a BIOS do seu computador para desligar o CD.
2. Coloque o CD na unidade e reinicie o computador.
3. Aguarde que o ecrã do BitDefender apareça e seleccione **Iniciar CD de Recuperação do BitDefender** no idioma preferido.
4. Aguarde que o processo de arranque termine. Poderá demorar algum tempo.
5. Assim que estiver concluído o processo de arranque, as assinaturas do BitDefender são automaticamente actualizadas e é iniciada uma análise a todas as partições do disco rígido detectadas.

   As partições do seu disco rígido irão aparecer no ambiente de trabalho. Para ver o conteúdo de um disco numa janela semelhante ao Explorador do Windows, faça duplo-clique.

   Nota
   Ao trabalhar com o CD de Recuperação do BitDefender, estará a trabalhar com nomes de partição do tipo Linux. Os discos que não forem etiquetados no Windows aparecerão como `[LocalDisk-0]`, correspondendo, provavelmente, à `(C:)` partição de tipo Windows, `[LocalDisk-1]` correspondendo a `(D:)` e assim sucessivamente.

6. Ligue o dispositivo amovível a uma porta USB do seu computador.Brevemente aparecerá uma janela a mostrar o conteúdo do dispositivo.
7. Pode copiar ficheiros e pastas normalmente, tal como no ambiente do Windows.

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção “*Apoio*” (p. 138).

## 30.2. O Que Fazer Se o BitDefender Encontrar Vírus No Seu Computador?

Pode verificar se há um vírus no seu computador de uma das seguintes formas:

- O BitDefender analisou o seu computador e encontrou itens infectados.
- Um alerta de vírus avisa que o BitDefender bloqueou um ou vários vírus no seu computador.

Nestas situações, actualize o BitDefender para se certificar que tem as assinaturas de malware mais recentes e realize uma Análise Minuciosa ao Sistema.

Assim que a análise minuciosa terminar, seleccione a acção pretendida para os itens infectados (Desinfectar, Eliminar, Mover para a Quarentena).

Atenção
Se suspeitar que o ficheiro faz parte do sistema operativo do Windows ou que não é um ficheiro infectado, não siga estes passos e contacte e Apoio ao Cliente do BitDefender assim que possível.

Se não for possível efectuar a acção seleccionada e o relatório da análise indicar uma infecção que não foi possível eliminar, tem de remover o(s) ficheiro(s) manualmente:

**O primeiro método pode ser utilizado no modo Normal**:

1. Desactive a protecção antivírus em tempo real do BitDefender.Para saber como fazer isto, consulte "*Como Posso Activar/Desactivar a Protecção Em Tempo Real*" (p. 147).
2. Mostrar objectos ocultos no Windows.Para saber como fazer isto, consulte "*Como Posso Mostrar Objectos Ocultos no Windows?*" (p. 148).
3. Procure a localização do ficheiro infectado (veja no relatório da análise) e elimine-o.
4. Active a protecção antivírus em tempo real do BitDefender.

**No caso de o primeiro método falhar ao remover a infecção, siga os seguintes passos**:

1. Reinicie o seu sistema e inicie sessão no Modo de Segurança.Para saber como fazer isto, consulte "*Como Posso Reiniciar no Modo de Segurança?*" (p. 146).
2. Mostrar objectos ocultos no Windows.
3. Procure a localização do ficheiro infectado (veja no relatório da análise) e elimine-o.
4. Reinicie o seu sistema e inicie sessão no modo normal.

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção "*Apoio*" (p. 138).

## 30.3. Como Posso Limpar o Vírus de um Arquivo?

Um arquivo é um ficheiro ou um conjunto de ficheiros comprimidos num formato especial para reduzir o espaço no disco necessário para armazenar os ficheiros.

Alguns destes formatos são formatos livres, possibilitando ao BitDefender a opção de analisar o conteúdo e aplicar as acções adequadas para os remover.

Outros formatos de arquivo estão parcial ou totalmente fechados, mas o BitDefender só pode detectar a presença de vírus no interior, mas não pode aplicar outras acções.

Se o BitDefender avisar que foi detectado um vírus dentro de um arquivo e não estiver disponível uma acção, significa que não é possível remover o vírus devido a restrições nas definições de permissão do arquivo.

Pode limpar um vírus armazenado num arquivo da seguinte forma:

1. Identifique o arquivo que contém o vírus realizando uma Análise Minuciosa ao Sistema.
2. Desactive a protecção antivírus em tempo real do BitDefender.
3. Vá à localização do arquivo e descomprima-o com uma aplicação de arquivo, como o WinZip.
4. Identifique e elimine o ficheiro infectado.
5. Elimine o arquivo original de modo a garantir que a infecção é totalmente removida.
6. Comprima novamente os ficheiros num novo arquivo com uma aplicação de arquivo, como o WinZip.
7. Active a protecção antivírus em tempo real do BitDefender e execute uma análise minuciosa ao sistema para se certificar que não há outras infecções no sistema.

Nota

É importante saber que um vírus armazenado num arquivo não é uma ameaça imediata ao seu sistema pois o vírus tem de ser descomprimido e executado de modo a infectar o seu sistema.

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção "*Apoio*" (p. 138).

## 30.4. Como Posso Limpar o Vírus de um Arquivo de Correio Electrónico?

O BitDefender também pode identificar vírus em bases de dados de correio electrónico e arquivos de correio electrónico armazenados no disco.

Por vezes, é necessário identificar a mensagem infectada com a informação fornecida no relatório da análise, e elimine-o manualmente.

Pode limpar um vírus armazenado num arquivo de correio electrónico da seguinte forma:

1. Analisar a base de dados do correio electrónico com o BitDefender.
2. Desactive a protecção antivírus em tempo real do BitDefender.
3. Abra o relatório da análise e utilize a informação de identificação (Assunto, De, Para) das mensagens infectadas para localizá-las no cliente de correio electrónico.

4. Elimine as mensagens infectadas.A maioria dos clientes de correio electrónico move a mensagem eliminada para uma pasta de recuperação, a partir da qual pode ser recuperada.Deve certificar-se que a mensagem também é eliminada desta pasta de recuperação.
5. Compactar a pasta com a mensagem infectada.
   - No Outlook Express:No menu Ficheiro, clique em Pasta e, depois em Compactar Todas as Pastas.
   - No Microsoft Outlook:No menu Ficheiro, clique em Gestão de Ficheiros de Dados.Seleccione os ficheiros das pastas (.pst) que pretende compactar e clique em Definições.Clique em Compactar.
6. Active a protecção antivírus em tempo real do BitDefender.

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção "*Apoio*" (p. 138).

## 30.5. Como Posso Analisar o Computador no Modo de Segurança?

A análise manual BitDefender deixa-o analisar uma determinada pasta ou partição do disco sem ter de criar uma tarefa de análise.

Esta ferramenta foi desenhada para ser usada quando o Windows está a correr em Modo de Segurança.

Se o seu sistema está infectado com um vírus que não pode ser removido no modo normal, pode tentar remover o vírus iniciando o Windows em Modo de Segurança e analisando cada partição do disco rígido usando a Análise Manual BitDefender.

Para saber como pode aceder ao Modo de Segurança, consulte "*Como Posso Reiniciar no Modo de Segurança?*" (p. 146).

1. Para analisar o seu computador com a Análise Manual do BitDefender, siga o seguinte caminho a partir do menu Iniciar do Windows: **Iniciar → Todos os Programaas → BitDefender 2011 → Análise Manual BitDefender**.
2. Clique em **Adicionar Pasta** para seleccionar o alvo da análise. Aparecerá uma nova janela.
3. Seleccione o alvo da análise :
   - para analisar o seu ambiente de trabalho, seleccione apenas **Ambiente de Trabalho**.
   - para analisar a partição do disco rígido completa, seleccione-a no **Meu Computador**.
   - para analisar uma determinada pasta, localize-a e seleccione-a.
4. Clique em **Ok** e **Continuar** para iniciar a análise.

5. Siga o assistente de Análise Antivírus para completar a análise.

## 30.6. O Que Fazer Se o BitDefender Identificou um Ficheiro Limpo como Infectado?

Há situações em que o BitDefender assinala erradamente um ficheiro legítimo como sendo uma ameaça (um falso positivo).Para corrigir este erro, adicione o ficheiro à área de Exclusões do BitDefender:

1. Desactive a protecção antivírus em tempo real do BitDefender.Para saber como fazer isto, consulte "*Como Posso Activar/Desactivar a Protecção Em Tempo Real*" (p. 147).
2. Mostrar objectos ocultos no Windows.Para saber como fazer isto, consulte "*Como Posso Mostrar Objectos Ocultos no Windows?*" (p. 148).
3. Restaurar o ficheiro da área de Quarentena.
4. Insira o ficheiro na área de Exclusões.
5. Active a protecção antivírus em tempo real do BitDefender.

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção "*Apoio*" (p. 138).

## 30.7. Como Limpar os Ficheiros Infectados da Informação de Volume de Sistema

A pasta de Informação de Volume do Sistema é uma zona no seu disco rígido criada pelo Sistema Operativo e utilizada pelo Windows para armazenar informações essenciais relacionadas com a configuração do sistema.

Os motores do BitDefender podem detectar qualquer ficheiro infectado armazenado na Informação de Volume de Sistema mas, sendo esta uma área protegida, poderá não conseguir removê-lo.

Os ficheiros infectados detectados nas pastas do Restauro do Sistema aparecerão no relatório da análise da seguinte forma:

```
?:\Informação de Volume de Sistema\_restore{B36120B2-BA0A-4E5D-…
```

Para remover total e imediatamente o(s) ficheiro(s) infectado(s) do armazém de dados, desactive e reactive o recurso do Restauro do Sistema.

Se o Restauro do Sistema estiver desactivado, todos os pontos de restauro são removidos.

Quando o Restauro do Sistema é novamente activado, são criados novos pontos de restauro consoante as necessidades do agendamento e de eventos.

Para desactivar o Restauro do Sistema, siga os seguintes passos:

- **Para o Windows XP:**
  1. Siga este caminho: **Iniciar** → **Todos os Programas** → **Acessórios** → **Ferramentas do Sistema** → **Restauro do Sistema**
  2. Clique em **Definições do Restauro do Sistema**, na lado esquerdo da janela.
  3. Seleccione a caixa **Desactivar o Restauro do Sistema** em todas as unidades e clique em **Aplicar**.
  4. Quando receber a notificação que todos os Pontos de Restauro serão eliminados, clique em **Sim** para continuar.
  5. Para activar o Restauro do Sistema, desmarque a caixa **Desactivar o Restauro do Sistema** em todas as unidades e clique em **Aplicar**.
- **Para o Windows Vista:**
  1. Siga o seguinte caminho: **Iniciar** → **Painel de Controlo** → **Sistema e Manutenção** → **Sistema**
  2. No painel da esquerda, clique em **Protecção do Sistema**.

     Se lhe for pedida a palavra-passe de administrador ou a confirmação, escreva a palavra-passe ou dê a confirmação.
  3. Para desactivar a Restauração do Sistema, desmarque as caixas de selecção de cada unidade e clique em **Ok**.
  4. Para activar o Restauro do Sistema, desmarque as caixas de selecção de cada unidade e clique em **Ok**.
- **Para o Windows 7:**
  1. Clique em **Iniciar**, clique com o botão direito em **Computador** e clique em **Propriedades**.
  2. Clique na hiperligação da **Protecção do sistema** no painel da esquerda.
  3. Nas opções da **Protecção do Sistema**, seleccione a letra de cada unidade e clique em **Configurar**.
  4. Seleccione **Desactivar protecção do sistema** e clique em **Aplicar**.
  5. Clique em **Eliminar**, clique em **Continuar** quando pedido e, depois, clique em **Ok**.

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção “*Apoio*” (p. 138).

## 30.8. O que são Ficheiros Protegidos por Palavra-Passe no Relatório de Análise?

Isto é apenas uma notificação que indica que o BitDefender detectou que estes ficheiros estão protegidos por palavra-passe ou por outra forma de encriptação.

Normalmente, os itens protegidos por palavra-passe são:

- Ficheiros que pertencem a outras solução de segurança.
- Ficheiros que pertencem ao sistema operativo.

Para analisar verdadeiramente os conteúdos, estes ficheiros têm de ser extraídos ou de outra forma descodificados.

Se estes conteúdos pudessem ser extraídos, o verificador em tempo real do BitDefender analisaria-os automaticamente para manter o seu computador protegido.Se pretende analisar esses ficheiros com BitDefender, terá de contactar o fabricante do produto para receber mais informações sobre esses ficheiros.

Recomendamos que ignore estes ficheiros pois não constituem uma ameaça ao seu sistema.

## 30.9. O Que São os Itens Ignorados no Relatório de Análise?

Todos os ficheiros que aparecem como Ignorados no relatório de análise estão limpos.

Para um melhor desempenho, o BitDefender não analisa ficheiros que não tenham sido alterados desde a última análise.

## 30.10. O que são os Ficheiros Sobre-Comprimidos no Relatório de Análise?

Os itens sobre-comprimidos são elementos que não puderam ser extraídos pelo motor de análise ou elementos para os quais a desencriptação levaria demasiado tempo, tornando o sistema instável.

Sobre-comprimido significa que o BitDefender não realizou a análise a esse arquivo pois a descompactação iria consumir demasiados recursos do sistema. O conteúdo será analisado aquando o acesso em tempo real, se necessário.

## 30.11. Porque é que o BitDefender eliminou automaticamente um ficheiro infectado?

Se for detectado um ficheiro infectado, o BitDefender tentará automaticamente desinfectá-lo.Se a desinfecção falhar, o ficheiro é movido para a quarentena de modo a restringir a infecção.

Para determinados tipos de malware, a desinfecção não é possível por o ficheiro detectado ser totalmente malicioso. Nestes casos, o ficheiro infectado é eliminado do disco.

Este é, normalmente, o caso de ficheiros de instalação que são transferidos de sítios de Internet suspeitos.Se se encontrar numa situação assim, transfira o ficheiro de instalação do sítio de Internet do fabricante ou de outro sítio fiável.

# 31. Apoio

A BitDefender esforça-se por fornecer aos seus clientes um nível de suporte rápido e eficaz.Se encontrar algum problema ou se tiver alguma questão sobre o nosso produto BitDefender, pode utilizar vários recursos em linha para encontrar rapidamente uma solução ou resposta.Ou, se preferir, pode contactar a equipa de Apoio ao Cliente da BitDefender. Os nossos técnicos de apoio responderão atempadamente às suas questões e dar-lhe-ão a ajuda que precisar.

## 31.1. Recursos Em Linha

Estão disponíveis vários recursos em linha para o ajudar a resolver problemas e a responder a questões relacionados com o BitDefender.

- Base de Conhecimento do BitDefender:http://www.bitdefender.com/help
- Fórum de Suporte BitDefender:http://forum.bitdefender.com
- o portal de segurança informática Malware City:http://www.malwarecity.com
- os Tutoriais

Também pode utilizar o seu motor de busca favorito para saber mais sobre a segurança de computadores, os produtos BitDefender e a empresa.

### 31.1.1. Base de Conhecimento do BitDefender

A BitDefender Knowledge Base é um repositório de informação on-line acerca dos produtos BitDefender. Armazena, num formato de relatório facilmente acessível, os resultados das actividades de reparação de erros por parte da equipe técnica do suporte BitDefender e da equipe de desenvolvimento, isto juntamente com artigos gerais acerca de prevenção de vírus, a administração de soluções BitDefender e explicações pormenorizadas, e muitos outros artigos.

A BitDefender Knowledge Base encontra-se aberta ao público e pode ser utilizada gratuitamente. Esta abundância de informação é uma outra forma de dar aos clientes BitDefender o conhecimento e o aprofundamento que eles necessitam. Todos os pedidos de informação ou relatórios de erro válidos originários de clientes BitDefender são incluídos na BitDefender Knowledge Base, como relatórios de reparação de erros, ou artigos informativos como suplementos aos ficheiros de ajuda dos produtos.

A BitDefender Knowledge Base encontra-se disponível a qualquer altura em http://kb.bitdefender.com.

### 31.1.2. Fórum de Suporte BitDefender

O Fórum de Suporte do BitDefender proporciona aos utilizadores do BitDefender uma forma fácil de obter ajuda e ajudar os outros.

Se o seu produto BitDefender não estiver a funcionar correctamente, se não conseguir remover certos vírus do seu computador ou se tiver alguma questão sobre a forma como opera, coloque o seu problema ou a sua questão no fórum.

Os técnicos de apoio da BitDefender supervisionam o fórum, à espera de novas mensagens para fornecer ajuda. Também pode receber uma resposta ou solução de um utilizador mais experiente do BitDefender.

Antes de publicar o seu problema ou questão, por favor pesquise o fórum por um tópico semelhante ou relacionado.

O Fórum de Suporte do BitDefender está disponível em http://forum.bitdefender.com, em 5 idiomas diferentes: inglês, alemão, francês, espanhol e romeno.Clique na hiperligação **Protecção Casa & Casa/Escritório** para aceder à secção dedicada aos produtos de consumidor.

### 31.1.3. Portal Malware City

O portal Malware City é uma excelente fonte de informações relacionadas com segurança informática. Aqui, pode ficar a conhecer as várias ameaças a que o seu computador fica exposto quando ligado à Internet (malware, phishing, spam, cibercriminosos).Um dicionário útil que ajuda a compreender os termos de segurança informática que não conhece.

Os novos artigos são publicados regularmente para o manter actualizado sobre as últimas ameaças descobertas, as actuais tendências de segurança e outras informações sobre a indústria de segurança informática.

A página de Internet do Malware City é http://www.malwarecity.com.

### 31.1.4. Tutoriais

Os tutoriais vão orientá-lo passo-a-passo na configuração do produto.São criadas de forma simples e directa para passar a mensagem.

O objectivo mais importante é garantir uma experiência agradável providenciando informações básicas e intermédias sobre os princípios de segurança, como configurar e utilizar o BitDefender.

O objectivo principal é eliminar a necessidade de obter ajuda especializada com os tutoriais que fornecem informações específicas sobre como utilizar e configurar o BitDefender.

Por exemplo, em vez de telefonar ao apoio da BitDefender para receber instruções ou tentar seguir procedimentos complicados, pode ver e seguir os passos apresentados nos tutoriais.

## 31.2. Pedir Ajuda

A secção **Resolução de Problemas e Obter Ajuda** providencia a informação necessária relativamente às incidências mais frequentes que poderá encontrar ao utilizar este produto.

Se não encontrar a solução para o seu problema nos recursos disponibilizados, pode contactar-nos directamente:

- “Contacte-nos Directamente Do Seu Produto BitDefender” (p. 140)
- “Contacte-nos através da nossa Base de Conhecimento Em Linha” (p. 141)

Importante

Para contactar o Apoio ao Cliente da BitDefender tem de ter a conta BitDefender activada.Para mais informação, por favor consulte o “*Registo e a Minha Conta*” (p. 47).

### Contacte-nos Directamente Do Seu Produto BitDefender

Se possuir uma ligação activa à Internet, pode contactar o apoio do BitDefender directamente a partir do interface do produto (da janela do programa).

Para pedir ajuda, pode utilizar o Suporte Integrado disponível no produto.

Para utilizar o Suporte Integrado, siga os seguintes passos:

1. Abrir o BitDefender.
2. Clique na hiperligação **Ajuda e Suporte**, localizada no canto inferior direito da janela.
3. Agora tem duas opções:
   - Inicie uma procura na nossa base de dados para encontrar a informação que precisa.
   - Seleccione o departamento consoante o problema encontrado.

     **Apoio ao cliente** trata de questões de aquisições, licenças, reembolsos ou renovações.

     **Apoio técnico** inclui incidências relacionados com o próprio produto e respectiva operacionalidade.

     **Luta contra malware** aborda incidências relacionadas com vírus.
4. Leia os artigos ou os documentos e experimente as soluções propostas.
5. Se a solução não resolver o problema, utilize a hiperligação no artigo para iniciar a Ferramenta de Suporte.
6. Introduza o seu endereço electrónico, seleccione o departamento e escreva uma breve descrição do problema.

Clique **Seguinte**.

7. Por favor, aguarde alguns minutos enquanto o BitDefender recolhe as informações relacionadas com o produto. Esta informação irá ajudar os nossos engenheiros a encontrar uma solução para o seu problema.

   Clique **Seguinte**.

8. Clique em **Concluir** para enviar as informações ao Departamento de Apoio ao Cliente da BitDefender. Será contactado assim que possível.

## Contacte-nos através da nossa Base de Conhecimento Em Linha

Se não conseguir aceder às informações necessárias com o produto BitDefender, por favor consulte a nossa base de conhecimento em linha:

1. Vá para http://www.bitdefender.com/help.A BitDefender Knowledge Base possui inúmeros artigos que contêm soluções para incidências relacionadas com o BitDefender.
2. Procure na BitDefender Knowledge Base os artigos que lhe poderão dar a solução para o seu problema.
3. Leia os artigos ou os documentos e experimente as soluções propostas.
4. Se a solução não resolver o problema, utilize a hiperligação no artigo para contactar o Apoio Técnico BitDefender.
5. Contacte o suporte BitDefender por e-mail, chat ou telefone.

# 32. Contactos

Comunicação eficiente é a chave de um negócio bem-sucedido. Durante os últimos 10 anos a BITDEFENDER estabeleceu uma reputação indiscutível ao exceder as expectativas dos clientes e parceiros, ao procurar constantemente melhorar a comunicação. Por favor não hesite em contactar-nos acerca de qualquer questão ou assunto que nos queira colocar.

## 32.1. Endereços Web

Departmento Comercial: comercial@bitdefender.pt
Suporte Técnico:www.bitdefender.com/help
Documentação: documentation@bitdefender.com
Programa de Parcerias: partners@bitdefender.com
Marketing: marketing@bitdefender.com
Contactos Imprensa: pr@bitdefender.com
Oportunidades de Trabalho: jobs@bitdefender.com
Submeter Vírus: virus_submission@bitdefender.com
Submeter Spam: spam_submission@bitdefender.com
Relatórios de Abusos: abuse@bitdefender.com
Sítio de Internet do produto:http://www.bitdefender.com
Arquivos ftp do produto:ftp://ftp.bitdefender.com/pub
Distribuidores locais:http://www.bitdefender.com/site/Partnership/list/
Base de Conhecimento do BitDefender:http://kb.bitdefender.com

## 32.2. Distribuidores Locais

Os distribuidores locais BitDefender estão preparados para responder a quaisquer dúvidas relacionadas com as suas áreas de operação, quer sejam comerciais ou assuntos gerais.

Para encontrar um distribuidor BitDefender no seu país:

1. Vá para http://www.bitdefender.com/site/Partnership/list/.
2. A informação de contacto dos distribuidores locais BitDefender deve ser automaticamente apresentada. Se isto não acontecer, utilize o recurso de Localização de Parceiros no menu do lado esquerdo para seleccionar a área e o país de residência.
3. Se não encontrar um distribuidor BitDefender no seu país, não hesite em contactar-nos por correio electrónico através do endereço sales@bitdefender.com.Por favor, escreva a sua mensagem em inglês para podermos responder imediatamente.

## 32.3. Escritórios BitDefender

Os escritórios BitDefender estão preparados para responder a quaisquer perguntas respeitantes às suas áreas de operação, quer sejam questões comerciais e de assuntos gerais. Os seus respectivos endereços e contactos estão listados abaixo.

### E.U.A.

**BitDefender, LLC**
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Telefone (office&sales): 1-954-776-6262
Vendas: sales@bitdefender.com
Suporte Técnico: http://www.bitdefender.com/help
Web: http://www.bitdefender.com

### UK e Irlanda

Business Centre 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
Endereço electrónico: info@bitdefender.co.uk
Telefone: +44 (0) 8451-305096
Vendas: sales@bitdefender.co.uk
Suporte Técnico: http://www.bitdefender.com/help
Web: http://www.bitdefender.co.uk

### Alemanha

**BitDefender GmbH**
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Escritório: +49 2301 91 84 222
Vendas: vertrieb@bitdefender.de
Suporte Técnico: http://kb.bitdefender.de
Web: http://www.bitdefender.de

### Espanha

**BitDefender España, S.L.U.**
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
Fax: +34 93 217 91 28
Telefone: +34 902 19 07 65

Vendas: comercial@bitdefender.es
Suporte Técnico: www.bitdefender.es/ayuda
Website: http://www.bitdefender.es

## Roménia

**BITDEFENDER SRL**
West Gate Park, Building H2, 24 Preciziei Street
Bucharest
Fax: +40 21 2641799
Telefone Comercial: +40 21 2063470
E-mail Vendas: sales@bitdefender.ro
Suporte Técnico: http://www.bitdefender.ro/suport
Website: http://www.bitdefender.ro

# 33. Informações Úteis

Este capítulo apresenta alguns procedimentos importantes que tem de considerar antes de começar a fazer o diagnóstico de um problema técnico.

Resolver um problema técnico do BitDefender requer alguns conhecimentos do Windows, por isso os passos seguintes estão quase totalmente relacionados com o sistema operativo do Windows.

## 33.1. Como Posso Remover Outras Soluções de Segurança?

A principal razão para utilizar uma solução de segurança é proporcionar protecção e segurança aos seus dados.Mas o que acontece quando tem mais do que um produto de segurança no mesmo sistema?

Quando utiliza mais do que uma solução de segurança no mesmo computador, o sistema torna-se instável.O instalador do BitDefender Antivirus Pro 2011 detecta automaticamente outros programas de segurança e oferece-lhe a opção de os desinstalar.

Se não tiver removido as outras soluções de segurança durante a instalação inicial, siga os seguintes passos:

- Para o **Windows XP**:
  1. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Adicionar/Remover Programas**.
  2. Aguarde alguns momentos até que a lista do software instalado seja apresentada.
  3. Encontre o nome do programa que pretende remover e seleccione **Remover**.
  4. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.
- Para o **Windows Vista** e o **Windows 7**:
  1. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.
  2. Aguarde alguns momentos até que a lista do software instalado seja apresentada.
  3. Encontre o nome do programa que pretende remover e seleccione **Desinstalar**.
  4. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

Se não conseguir remover as outras soluções de segurança do seu sistema, obtenha a ferramenta de desinstalação do sítio de Internet do fornecedor ou contacte-o directamente para receber instruções de desinstalação.

## 33.2. Como Posso Reiniciar no Modo de Segurança?

O Modo de Segurança é um modo operativo de diagnóstico, utilizado principalmente para detectar e resolver problemas que estejam a afectar o funcionamento normal do Windows.As causas destes problemas vão desde a incompatibilidade de controladores a vírus que impedem o arranque normal do Windows.No Modo de Segurança funcionam apenas algumas aplicações e o Windows só carrega os controladores básicos e os componentes mínimos do sistema operativo.É por isso que a maioria dos vírus está inactiva quando o Windows está no Modo de Segurança e podem ser facilmente removidos.

Para iniciar o Windows no Modo de Segurança:

1. Reinicie o computador.
2. Prima a tecla **F8** várias vezes antes de o Windows iniciar para aceder ao menu de arranque.
3. Seleccione **Modo de Segurança** no menu de arranque e prima **Enter**.
4. Aguarde enquanto o Windows é iniciado no Modo de Segurança.
5. Este processo termina com uma mensagem de confirmação.Clique em **Ok** para aceitar.
6. Para iniciar o Windows normalmente, basta reiniciar o sistema.

## 33.3. Estou a Utilizar uma Versão de 32 ou 64 Bit do Windows?

Para saber se tem um sistema operativo de 32 bit ou 64 bit, siga os seguintes passos:

- Para o **Windows XP**:
  1. Clique em **Iniciar**.
  2. Localize o **Meu Computador** no menu **Iniciar**.
  3. Clique com o botão direito em **Meu Computador** e seleccione **Propriedades**.
  4. Se estiver indicada a **Edição x64** na secção **Sistema**, está a executar a versão de 64 bit do Windows XP.

     Se não estiver indicada a **Edição x64**, está a executar a versão de 32 bit do Windows XP.
- Para o **Windows Vista** e o **Windows 7**:
  1. Clique em **Iniciar**.
  2. Localize o **Computador** no menu **Iniciar**.
  3. Clique com o botão direito em **Computador** e seleccione **Propriedades**.
  4. Procure na secção **Sistema** a informação sobre o seu sistema.

## 33.4. Como Posso Encontrar as Minhas Definições de Proxy?

Para encontrar estas definições, siga os seguintes passos:

- Para o Internet Explorer 8:
  1. Abra o Internet Explorer.
  2. Seleccione **Instrumentos** > **Opções de Internet**.
  3. No separador **Ligações** clique em **Definições LAN**.
  4. Na secção **Utilizar um servidor proxy para LAN** poderá encontrar p **Endereço** e a **Porta** do proxy.
- Para o Mozilla Firefox 3.6:
  1. Abra o Firefox.
  2. Seleccione **Instrumentos** > **Opções**.
  3. No separador **Avançadas**, abra o separador **Rede**.
  4. Clique em **Definições**.
- Para Opera 10.51:
  1. Abra o Opera.
  2. Seleccione **Recursos** > **Preferências**.
  3. No separador **Avançadas**, abra o separador **Rede**.
  4. Clique no botão **Servidores Proxy** para abrir a caixa de diálogo das definições proxy.

## 33.5. Como Posso Remover Totalmente o BitDefender?

Siga estes passos para remover correctamente o BitDefender:

1. Vá a www.bitdefender.com/uninstall e descarregue a ferramenta de desinstalação para o seu computador.
2. Execute a ferramenta de desinstalação com direitos de administrador.
3. Reinicie o seu computador.

## 33.6. Como Posso Activar/Desactivar a Protecção Em Tempo Real

O BitDefender providencia uma protecção contínua e em tempo-real, contra todo o tipo de ameaças de malware ao analisar os ficheiros acedidos, e as comunicações feitas através de aplicações de software de Mensagens Instantâneas (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

Normalmente, a protecção em tempo real do BitDefender está activada e não deve ser desligada.

Quando tentar resolver um problema ou remover um vírus, poderá ter de desactivar a protecção em tempo real. Estes dizem respeito a uma das seguintes situações:

- Um problema de abrandamento com o sistema após a instalação do BitDefender
- Um problema com um programa ou uma aplicação após a instalação do BitDefender
- Mensagens de erro que poderão aparecer pouco depois da instalação do BitDefender

Siga os seguintes passos para poder activar/desactivar temporariamente a protecção em tempo real:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Antivirus** > **Escudo**.
3. Desmarque a caixa **A protecção em tempo real está activada** para desactivar temporariamente a protecção antivírus (ou seleccione-a se pretende activar a protecção).
4. Tem de confirmar a sua escolha seleccionando no menu durante quanto tempo pretende desactivar a protecção em tempo real.

Nota

Os passos para desactivar a protecção em tempo real no BitDefender devem ser utilizados como uma solução temporária e apenas durante um curto período.

## 33.7. Como Posso Mostrar Objectos Ocultos no Windows?

Estes passos são úteis nos casos de malware e tiver de encontrar e remover os ficheiros infectados, que poderão estar ocultos.

Siga os seguintes passos para mostrar objectos ocultos no Windows:

1. Clique em **Iniciar**, vá ao **Painel de Controlo** e seleccione **Opções de Pastas**.
2. Abra o separador **Ver**.
3. Seleccione **Mostrar conteúdo das pastas de sistema** (apenas para o Windows XP).
4. Seleccione **Mostrar ficheiros e pastas ocultos**.
5. Desmarque **Ocultar extensões de ficheiros nos tipos de ficheiro conhecidos**.
6. Desmarque **Ocultar ficheiros protegidos do sistema operativo**.
7. Clique em **Aplicar** e depois em **Ok**.

# Glossário

**ActiveX**

O ActiveX é um modelo de escrita de programas, para que outros programas e o sistema operativo o possam chamar. A tecnologia do ActiveX é usada com o Microsoft Internet Explorer para criar páginas da Web interactivas, que parecem e compartam-se como programas de computador, em vez de páginas estácticas. Com o ActiveX, os utilizadores podem efectuar perguntas ou responder a questões, usando botões para carregar, e interagir de outras formas com a página da Web. Os controlos do ActiveX são frequentemente escritos utilizando o Visual Basic.

O Active X é notável para um leque completo de controlos de segurança; os especialistas de segurança dos computadores desencorajam o seu uso na Internet.

**Adware**

O adware é com frequência combinado com uma aplicação hospedeira que é fornecida sem custo desde que o utilizador concorde em aceitar o adware. Por causa de as aplicações adware serem normalmente instaladas após o utilizador concordar com uma licença de uso que define o propósito da aplicação, nenhuma ilegalidade é na verdade cometida.

No entanto, anúncios tipo pop-up podem tornar-se bastante incomodativos, e em alguns casos podem mesmo degradar a performance do sistema. Também, a informação que algumas dessas aplicações recolhem podem causar algumas preocupações de privacidade aos utilizadores que não estão completamente conscientes dos termos da licença de uso.

**Arquivo**

Um disco, cassete, ou directório que contém ficheiros que foram armazenados.

Um ficheiro que contém um ou mais ficheiros num formato comprimido.

**Porta das traseiras**

Um buraco na segurança de um sistema deliberadamente deixado ao acaso pelos desenhadores e protectores. A motivação para tais buracos não é sempre sinistra; alguns sistemas operativos, por exemplo, saem fora das caixas com contas priveligiadas, intencionadas para o uso no terreno por técnicos de serviço ou pelo vendedor dos programas de manutenção.

**Sector de saída**

Um sector no início de cada disco que identifica a arquitectura do disco (tamanho do sector, tamanho do grupo, e por aí a diante). Para discos de inicialização, o sector de saída também contém um progrma que carrega o sistema operativo.

**Vírus de saída**

Um vírus que infecta o sector de saída de um disco fixo ou de uma unidade de disquetes. A tentativa de retirar uma disquete infectada por um vírus de saída, irá causar a activação do vírus na memória. Sempre que iniciar o seu sistema daquele ponto, terá o vírus activo na memória.

**Navegador**

Diminuitivo para browser de internet, que é um software usado para localizar e mostrar páginas Web. Os dois mais populares browsers são o Netscape Navigator e o Microsoft Internet Explorer. Ambos são browsers gráficos, o que significa que eles tanto podem mostrar gráficos como texto. Em adição, a maioria dos browsers modernos podem apresentar informação multimédia, incluíndo som e vídeo, apesar de necessitarem de plug-ins para alguns formatos.

**Linha de comando**

Numa interface de linha do comando, o utilizador introduz comandos no espaço providenciado directamente no ecrã, usando a linguagem de comando.

**Cookie**

Desntro da indústria da Internet, as cookies são descritas como pequenos ficheiros, que contêm informação acerca de computadores individuais, que podem ser analizados e usados pelos publicitários para seguir o rasto online do seus interesses e gostos. Neste domínio, a tecnologia das cookies ainda está a ser desenvolvida e a sua intenção é encontrar alvos publicitários directamente do que disse serem os seus interesses. É uma espada de dois gumes para muitas pessoas, porque, por um lado aé eficiente e pertinente já que apenas vê anúncios do seu interesse. Por outro lado, envolve realmente "seguir o rasto" e "perseguir" onde vai e no que clica. Compreensivelmente, existe um debate acerca da privacidade e muitas pessoas sentem-se ofendidas ao terem a noção que estão a ser vistas como um "número SKU " (você sabe, o código de barras por detrás das embalagens que é verificado na mercearia). Enquanto este ponto de vista possa ser extremo, em alguns casos é preciso.

**Componente (drive) do disco**

É uma máquina que lê os dados do disco e escreve dados num disco.

Uma componente de disco rígido lê e escreve discos rígidos.

Uma componente de disquetes acede às disquetes.

As componentes do disco tanto podem ser internas (dentro do computador) ou externas (vêm numa caixa em separado que se liga ao computador).

**Transferir**

Para copiar dados (normalmente um ficheiro interno) de uma fonte principal para um aparelho periférico. O termo é frequentemente utilizado para descrever o processo de copiar um ficheiro de um serviço online para o seu próprio computador. Também se pode referir à cópia de um ficheiro de um servidor de ficheiros de rede, para um computador na rede.

**Correio electrónico**

Correio electrónico. É um serviço que envia mensagens em computadores via local ou redes globais.

**Eventos**

Uma acção ou ocorrência detectada por um programa. Os eventos podem ser acções do utilizador, tais como clicar no botão do rato ou carregar numa tecla, ou ocorrências do sistema, tais como ficar sem memórias.

**Falso positivo**

Ocorre quando o verificador identifica um ficheiro como infectado, quando na verdade ele não está.

**Extensão do nome do ficheiro**

A porção de um nome de ficheiro, que segue o ponto final, a qual indica o tipo de dados armazenados no ficheiro.

Muitos sistemas operativos usam extensões do nome do ficheiro, por ex. Unix, VMS, e MS-DOS. Elas são normalmente de uma a três letras. Os exemplos íncluem ".c" para C de código da fonte, ".ps" para PostEscrito, ".txt" para texto arbitrário.

**Heurístico**

Um método baseado na regra de identificar novos vírus. Este método de exame não se fia em assinaturas específicas de vírus. A vantagem do exame heurístico, é que não se deixa enganar por uma nova variante de um vírus existente. Contudo, pode reportar ocasionalmente códigos suspeitos em programas normais, gerando o chamado "falso positivo".

**IP**

Internet Protocol - Um rótulo de protocolo no protocolo TCP/IP séquito que é responsável dos endereços de IP, rotas, e a fragmentação e reabertura dos pacotes de IP.

**Java applet**

Um programa Java, o qual é desenhado para correr apenas numa página da web. Para usar uma applet numa página da web, you deverá especificar o nome da applet e o tamanho (comprimento e largura - em pixels) que a applet pode utilizar. Quando a página da web é acedida, o motor de busca descarrega a applet de um servidor e corre-a apenas na máquina do utilizador (o cliente). As applets diferem das aplicações, nas quais são administradas por um protocolo de segurança restrito.

Por exemplo, apesar de as applets correrem no cliente, elas não podem escrever nem lêr dados para a máquina do cliente. Adicionalmente, as applets são restritas para que possam apenas lêr e escrever dados provenientes do mesmo domínio, no qual elas são servidas.

**Macro vírus**

Um tipo de vírus de computador que está codificado como uma macro retido num documento. Muitas aplicações, tais como Microsoft Word e Excel, contêm poderosas linguagens macro.

Estas aplicações permitem-lhe reter uma macro num documento, e ter a macro pronta a ser executada sempre que o documento for aberto.

**Cliente de mail**

Um cliente de e-mail é uma aplicação que lhe permite enviar e receber e-mail.

**Memória**

Áreas internas de armazenamento no computador. O termo memória identifica armazenamento de dados que vêm na forma de chips, e a palavra armazenar é usada para a memória que existe em cassates ou discos. Todo o computador vem com uma certa quantidade de memótia física, normalmente referida como memória pricipal ou RAM.

**Não-heurístico**

Este método de exame confia em assinaturas de vírus especificas. A vantagem de um exame não-heurístico, é que ele não será induzido em erro pelo que possa parecer um vírus e não gera falsos alarmes.

**Programas compactados**

Um ficheiro num formato compactado. Muitos sistemas operativos e aplicações contêm comandos que lhe permitem compactar um ficheiro, para que ocupe menos memória. Por exemplo, suponha que tem um ficheiro de texto contendo dez espaços de caracteres consecutivos. Normalmente isto iria requerer dez de armazenamento.

Contudo, um programa que compacta ficheiros iria substituir o espaço dos caracteres por uma série-de-espaços de caracteres especial, seguida pelo número de espaços a ser substituidos. Neste caso, os dez espaços iriam requeres apenas dois bytes. Esta é apenas uma técnica de compactar, há muitas.

**Caminho**

As direcções exactas para um ficheiro num computador. Estas direcções são normalmente descritas por meios de preenchimento hierárquico do topo para baixo.

A rota entre dosi dados pontos, tal como os canais de comunicação entre dois.

**Phishing**

O acto de enviar um e-mail a um utilizador como sendo falsamente uma empresa legítima e estabelecida numa tentativa de levar o utilizador a providenciar informação privada que será utilizada para roubo. O e-mail leva o utilizador a visitar um site na Internet onde lhe é solicitado que actualize informação pessoa, tal como passwords e números de cartões de crédito, segurança social, e

números de contas bancárias, que a legítima organização já possui. O site Web, no entanto, é falso e está feito apenas para roubar a informação ao utilizador.

**Vírus polimórfico**

Um vírus que altera a sua forma com cada ficheiro que infecta. Dado que eles não têm uma consistência de patente binária, tais vírus são difíceis de identificar.

**Porta**

Uma interface num computador, à qual se liga um aparelho. Os computadores pessoais tendo vários tipos de portas. Internamente, existem várias portas para ligar componentes de disco, ecrãs, e tecladoss. Externamente, os computadores pessoais têm portas para ligar modems, impressoars, ratos, e outros aparelhos periféricos.

Nas redes TCP/IP e UDP, um ponto de fim para uma ligação lógica. O número da porta identifica o tipo da porta. Por exemplo, a porta 80 é usada para o tráfego HTTP.

**Ficheiro de reporte**

Um ficheiro que lista acções que tiveram ocurrência. O BitDefender um ficheiro de reporte que lista o caminho examinado, as pastas, o número de arquivos e ficheiros examinados, e quantos ficheiros suspeitos e infectados foram encontrados.

**Rootkit**

Um rootkit é um pacote de ferramentas de software que proporcionam um nível de acesso de administrador a um sistema. O termo foi usado em primeiro lugar nos sistemas operativos UNIX e referia-se a ferramentas recompiladas que proporcionavam aos intrusos direitos de administração, permitindo-lhes ocultar a sua presença de forma a não serem vistos pelos administradores do sistema.

O papel principal dos rootkits é ocultar processos, ficheiros, logins e registos. Eles também podem interceptar dados dos terminais, ligações de rede ou periféricos, se eles incorporarem o software para tal.

Os rootkits não são maliciosos por natureza. Por exemplo, os sistemas e mesmo algumas aplicações ocultam ficheiros críticos usando rootkits. No entanto, eles são essencialmente utilizados para ocultar malware ou para esconder a presença de um intruso no sistema. Quando combinados com o malware, os rootkits são uma grande ameaça à integridade e segurança de um sistema. Eles podem monitorizar tráfego, criar backdoors no sistema, alterar ficheiros e relatórios e evitarem ser detectados.

**Escrita**

Outro termo para macro ou ficheiro de porção, uma escrita é uma lista de comandos que podem ser executados sem a interacção do utilizador.

**Spam**

Lixo de correio electrónico ou lixo de avisos de newsgroups. É normalmente conhecido como correio não-solicitado.

**Spyware**

O estabelecimento de ligação à Internet do utilizador sem o seu conhecimento, normalmente para propósitos de publicidade. As aplicações de spyware são tipicamente adicionadas como um elemento oculto de programas freeware ou shareware que podem ser download a partir da Internet; no entanto salientamos que a maioria das aplicações freeware ou shareware não possuem spyware. Uma vez instalado, o spyware monitoriza a actividade do utilizador na Internet e transmite essa informação em background para alguém. O spyware pode também reunir informação acerca de endereços de e-mail e até mesmo passwords e números de cartões de crédito.

O spyware é similar a um cavalo-de-troia em que os utilizadores o instalam sem saberem, enquanto estão a instalar outra coisa qualquer. Uma forma comum de ser uma vítima de spyware é fazer download de determinado ficheiro peer-to-peer de produtos de swapping que se encontram actualmente disponíveis.

Para além destas questões de ética e privacidade, o spyware priva o utilizador de recursos de memória e também de largura de banda pois para enviar informação do utilizador para a fonte do spyware usa a ligação à Internet do utilizador. Por causa do spyware utilizar memória e recursos do sistema, as aplicações que estão a funcionar em background podem causar crashes no sistema ou uma grande instabilidade geral.

**Itens que começam a funcionar ao ínicio**

Qualquer ficheiro colocado nesta pasta, irá abrir quando o computador iniciar. Por exemplo, um ecrã que abra no ínicio, um ficheiro de som a ser tocado quando ligar inicialmente o computador, um lembrete, ou programas de aplicação podem ser itens que começam a funcionar ao iniciar o computador. Normalmente, é colocado um pseudónimo deste ficheiro nesta pasta, em vez do ficheiro em si próprio.

**Caixa do sistema**

Introduzido com o Windows 95, o tabuleiro do sistema está localizado na barra de tarefas do Windows (normalmente em baixo, junto ao relógio) e contém ícones em miniatura para um acesso fácil às funções do sistema, tais como fax, impressora, modem, volume, etc. Faça duplo-clique ou clique com o botão direito sobre o ícone para ver e aceder aos detalhes e controlos.

**TCP/IP**

Transmission Control Protocol/Internet Protocol - Um conjunto de protocolos de uma rede de trabalho abrangentemente usados Internet que permite comunicações ao londo de redes de computadores interconectadas com várias arquitecturas de hardware e vários sistemas operaticos. O TCP/IP ínclui padrões

de como os computadores comunicam e convenções para conectar redes e rotas de tráfego.

**Tróiano**

Um programa destrutivo que se mascara de aplicação benigna. Ao contrário dos vírus, os cavalos de Tróia não se replicam, mas podem ser tão destrutivos como os vírus. Um dos cavalos de Tróia mais incidente é o programa que promete ver-se livre dos vírus do seu computador, mas em vez disso introduz vírus no seu computador.

O termo provém de uma história da Ilíada de Homero, na qual os Gregos deram um cavalo gigante de Madeira aos seus inimigos, os Troianos, como uma oferta majestosa. Mas após os Troianos levarem o cavalo para dentro das muralhas da sua cidade, os soldados Gregos saíram para fora do cavalo e abriram os portões da cidade, permitindo que os seus compatriotas entrassem e dominassem Tróia.

**Actualização**

Uma nova versão de um produto de software ou hardware desenhada para substituir uma versão antiga do mesmo produto. Em adição, a instalação de rotina da actualização verifica se a versão anterior já está instalada no seu computador; se não estiver, não poderá instalar a actualização.

O BitDefender tem o seu próprio modulo de actualização que lhe permite verificar actualizações manualmente, ou permitir actualizar o produto automaticamente.

**Vírus**

Um programa ou um pedaço de código que é carregado no seu computador sem o seu conhecimento e decorre contra a sua vontade. A maioria dos vírus podem-se replicar. Todos os vírus de computação são feitos pelo Homem. Um simples vírus que se possa reproduzir a si próprio vezes sem conta, é relativamente fácil de fabricar. Mesmo um simples vírus é perigoso, porque usará rapidamente toda a memória disponível e levará o sistema a uma quebra. Ainda um mais perigoso tipo de vírus é aquele capaz de se transmitir ao longo das redes e ultrapassar sistemas de segurança.

**Definição de vírus**

A patente binária de um vírus, usada pelo programa de anti-vírus para detectar e eliminar os vírus.

**Minhoca**

Um programa que se propaga a si próprio ao longo de uma rede, reproduzindo-se à medida que avança. Não pode ligar-se sozinho a outros programas.